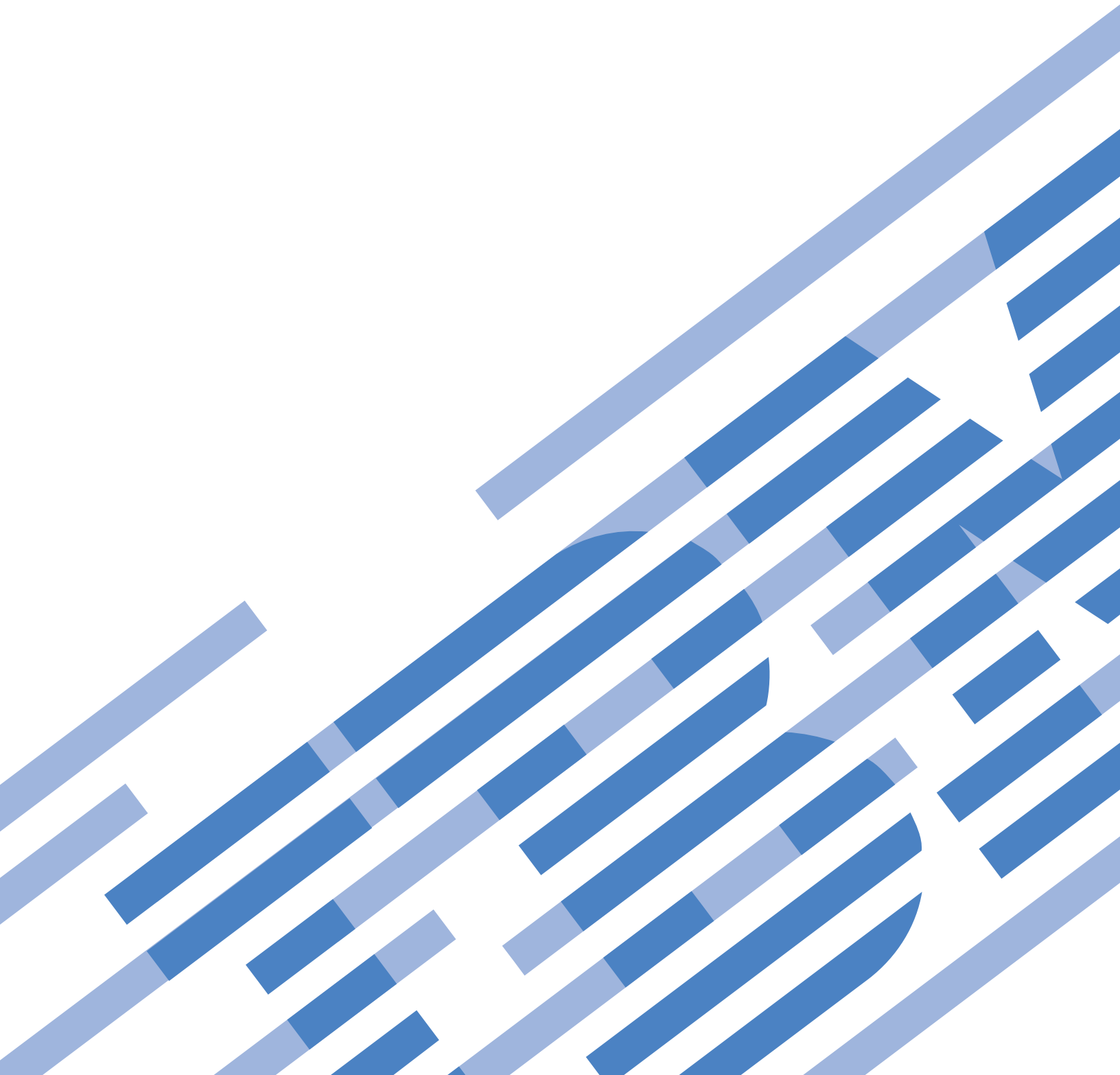




System z

Advanced Workload Analysis Reporter (IBM zAware) Guide

SC27-2623-01





System z

Advanced Workload Analysis Reporter (IBM zAware) Guide

SC27-2623-01

Note

Before using this information and the product it supports, read the information in “Safety” on page ix, Appendix E, “Notices,” on page 241 and *IBM Systems Environmental Notices and User Guide*, Z125-5823.

This edition, SC27-2623-01, applies to IBM zEnterprise System (zEnterprise). This edition replaces SC27-2623-00.

There might be a newer version of this document in a **PDF** file available on **Resource Link**. Go to <http://www.ibm.com/servers/resourcelink> and click **Library** on the navigation bar. A newer version is indicated by a lowercase, alphabetic letter following the form number suffix (for example: 00a, 00b, 01a, 01b).

© **Copyright IBM Corporation 2012, 2013.**

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

Contents

Figures v

Tables vii

Safety ix

Safety notices ix

World trade safety information ix

Laser safety information ix

Laser compliance ix

About this publication xi

Intended audience xi

Prerequisite and related information xi

Related HMC and SE information xi

How to use this publication xii

Accessibility xii

How to send your comments xiii

Summary of changes xv

**Part 1. Introduction to the IBM
System z Advanced Workload
Analysis Reporter (IBM zAware) . . . 1**

Chapter 1. Overview of IBM zAware . . . 3

**Chapter 2. Prerequisites for configuring
and using IBM zAware 11**

**Chapter 3. Project plan for configuring
and using IBM zAware 13**

**Part 2. Planning to configure IBM
zAware 17**

**Chapter 4. Planning your IBM zAware
environment 19**

**Chapter 5. Estimating data center
resource requirements 27**

Estimating processor and memory resources . . . 27

Planning network connections and capacity . . . 29

Planning persistent storage configuration and
capacity 35

Chapter 6. Planning for security 51

**Chapter 7. Planning to use the IBM
zAware GUI. 55**

Accessibility features for the IBM zAware GUI . . 56

**Chapter 8. Planning to create IBM
zAware models 57**

**Part 3. Configuring IBM zAware and
its monitored clients. 61**

**Chapter 9. Configuring network
connections and storage for the IBM
zAware partition. 63**

**Chapter 10. Configuring an image
profile for the IBM zAware partition . . 67**

**Chapter 11. Configuring storage,
security, and analytics for the IBM
zAware server 79**

**Chapter 12. Configuring z/OS
monitored clients to send data to the
IBM zAware server 91**

**Chapter 13. Creating an IBM zAware
model for new z/OS monitored clients . 99**

**Part 4. Managing and using the
IBM zAware server 107**

**Chapter 14. Viewing and using
analytical data to monitor and
diagnose system behavior. 109**

Using the Analysis page to monitor and diagnose
system behavior 109

Change Analysis Source window 115

The Analysis page in tabular format. 117

Using the Interval view to pinpoint the causes of
system anomalies 118

Select Nested Sort Attributes window 124

Time Line Summary window 125

Ignore Message Status window 126

Verifying planned system changes with IBM
zAware 127

**Chapter 15. Specifying security
settings for the IBM zAware GUI . . . 129**

Replacing the default SSL certificate 130

SSL Settings tab 131

Create Certificate Signing Request page . . . 132

View Last Generated Request page 133

Receive Certificate Authority Reply page . . . 133

| | |
|---|-----|
| Enabling LDAP authentication for IBM zAware users | 133 |
| LDAP Settings tab. | 135 |
| Assigning users or groups to a role | 137 |
| Role Mapping tab | 139 |
| Specifying the duration of a browser session | 141 |

Chapter 16. Managing IBM zAware operation and resources 143

| | |
|--|-----|
| Accessing your notifications | 143 |
| Assigning storage devices to IBM zAware | 143 |
| Adding and removing storage devices | 145 |
| Specifying settings for the analytics engine | 148 |
| Viewing the status of monitored clients. | 150 |
| System Status page | 150 |
| Starting and stopping data collection for your monitored systems | 153 |
| Monitoring processor and memory resources | 154 |
| Applying service updates for IBM zAware | 154 |
| Deactivating the IBM zAware partition | 155 |

Part 5. Advanced topics for managing IBM zAware 157

Chapter 17. Managing the training for monitored clients. 159

| | |
|--|-----|
| Understanding training periods and intervals | 159 |
| Viewing model dates | 161 |
| Excluding dates from a model. | 161 |
| Requesting training | 162 |
| Canceling training. | 164 |
| Managing ignored messages | 164 |
| Training Sets page. | 166 |
| Manage Model Dates page | 171 |
| Summary view | 171 |
| Calendar view | 173 |
| Manage Ignored Messages page | 175 |

Chapter 18. Collecting priming data for IBM zAware models 179

| | |
|---|-----|
| Assigning the priming data to a sysplex | 179 |
| Priming Data tab | 181 |

Chapter 19. Modifying the sysplex topology 183

| | |
|--|-----|
| Move Selected Systems window | 184 |
|--|-----|

Chapter 20. Setting up a local repository to secure access to the IBM zAware GUI 185

Chapter 21. Setting up multiple IBM zAware partitions for switchover situations 187

Chapter 22. Enabling system management products to use IBM zAware data 191

| | |
|---|-----|
| Integrating IBM zAware data into monitoring and alerting products | 191 |
| Viewing the IBM zAware GUI through z/OS Management Facility | 193 |

Chapter 23. Troubleshooting problems in the IBM zAware environment 195

Chapter 24. Reporting IBM zAware problems to IBM 199

Part 6. Appendixes 203

Appendix A. Summary of IBM zAware tasks and required IT skills, tools and information 205

Appendix B. Sample certificate authority (CA) reply. 209

Appendix C. Application Programming Interface (API) for monitoring products 213

| | |
|--|-----|
| API versioning | 213 |
| Syntax and description of a GET request for IBM zAware data. | 213 |
| XML for an LPAR request | 215 |
| XML for an INTERVAL request | 218 |

Appendix D. IBM zAware operational messages 225

Appendix E. Notices 241

| | |
|---------------------------------------|-----|
| Trademarks | 242 |
| Electronic emission notices | 242 |

Glossary 247

Index 253

Figures

| | | | |
|--|----|--|-----|
| 1. Elements of the Analysis page that help identify the problematic z/OS system | 4 | 19. Configuration process for the alternate IBM zAware server on a different host system | 45 |
| 2. Elements of the Analysis page that change the time interval display | 5 | 20. What happens when a switchover situation occurs | 47 |
| 3. Elements of the Interval view that provide details about unique messages | 6 | 21. LPAR image profile: Selecting the name of the IBM zAware partition to create a new image profile | 68 |
| 4. An IBM zAware partition running in a zEC12 CPC | 8 | 22. LPAR image profile: General characteristics with the IBM zAware mode | 69 |
| 5. An IBM zAware partition supporting clients in one zEC12 CPC and one z196 | 9 | 23. LPAR image profile: Processor characteristics | 70 |
| 6. System management products using IBM zAware analytical data | 10 | 24. LPAR image profile: Security characteristics | 73 |
| 7. Types of z/OS monitored clients connected to a IBM zAware partition in a zEC12 CPC | 20 | 25. LPAR image profile: Storage | 74 |
| 8. An IBM zAware configuration with two partitions, each supporting the clients in one of two physical sites | 22 | 26. LPAR image profile: Options | 75 |
| 9. Two IBM zAware partitions in one zEC12 CPC with multiple firewalls | 23 | 27. Adding a new network adapter using an IPv4 address | 76 |
| 10. An IBM zAware environment containing sysplexes that are split between two physical buildings | 25 | 28. LPAR image profile: zAware page | 77 |
| 11. Supported network connection options for the IBM zAware environment | 30 | 29. The landing page for IBM zAware | 81 |
| 12. Network connections for an IBM zAware partition supporting clients in two zEC12 CPCs | 31 | 30. A sample bar graph from the Analysis page display | 110 |
| 13. Configuration files for network connections | 32 | 31. A sample Analysis page | 112 |
| 14. DASD configuration for normal operations, with access for one z/OS partition only to back up IBM zAware data | 37 | 32. Date and time controls for the Analysis page | 114 |
| 15. Storage configuration for the IBM zAware server for normal operations and data replication | 39 | 33. A sample Change Analysis Source window | 115 |
| 16. What happens when an in-use storage device becomes unavailable | 41 | 34. A sample Analysis page in tabular format | 117 |
| 17. The Preserve data option on the Add and Remove Devices window | 42 | 35. A sample Interval view display | 119 |
| 18. DASD configuration for the primary IBM zAware server on one host system | 43 | 36. The Ignore Message Status window | 121 |
| | | 37. The Interval view Time Line in tabular (text-only) format | 122 |
| | | 38. Sample timeline for retraining IBM zAware to analyze data from a new application | 128 |
| | | 39. Training schedule for example 1 | 160 |
| | | 40. Training schedule for example 2 | 160 |
| | | 41. Features in the calendar widget | 172 |
| | | 42. Training Calendar | 174 |
| | | 43. The Manage Ignored Messages page | 176 |
| | | 44. Sample reply from a third-party certificate authority | 210 |
| | | 45. Illustration of required format for pasting into the GUI | 211 |

Tables

| | | | | | |
|-----|---|-----|-----|---|-----|
| 1. | List of feature codes for ordering IBM zAware | 11 | 29. | Fields displayed on the page before the CSR is generated | 132 |
| 2. | Required V1R13 PTFs for z/OS monitored clients | 12 | 30. | Fields displayed on the page after the CSR is generated | 133 |
| 3. | Planning checklist for the IBM zAware environment | 13 | 31. | Fields displayed on the View Last Generated Request page | 133 |
| 4. | Configuration checklist for the IBM zAware partition | 13 | 32. | General LDAP settings | 135 |
| 5. | Configuration checklist for the IBM zAware server and monitored clients | 14 | 33. | Group LDAP settings | 136 |
| 6. | Required V1R13 PTFs for z/OS monitored clients | 19 | 34. | Items displayed in the Role Mapping tab | 139 |
| 7. | Supported channel path types for the IBM zAware partition | 33 | 35. | Fields displayed in the Apply Role Mappings window | 140 |
| 8. | Task summary for network administrators | 34 | 36. | Fields on the Data Storage tab | 144 |
| 9. | Checklist for IBM zAware partition network settings | 34 | 37. | Columns in the Data Storage Devices table | 145 |
| 10. | Checklist for IBM zAware partition network adapters | 35 | 38. | Items displayed in the Add and Remove Devices window | 147 |
| 11. | Planning considerations and best practices for IBM zAware storage | 36 | 39. | Fields on the Analytics tab | 149 |
| 12. | Planning considerations and best practices for IBM zAware storage configuration | 48 | 40. | Field on the System Status page | 152 |
| 13. | Task summary for storage administrators | 50 | 41. | Columns in the zAware Monitored System Data Suppliers table | 153 |
| 14. | Checklist for Extended Count Key Data (ECKD) storage devices | 50 | 42. | Columns in the Monitored Systems table | 166 |
| 15. | Task summary for security administrators | 54 | 43. | Actions for monitored systems. | 169 |
| 16. | Supported channel path types for the IBM zAware partition | 64 | 44. | Fields in the Current Training Status Details section | 169 |
| 17. | Image profile: zAware partition values for the General page | 69 | 45. | Fields displayed in the Summary view for the next model | 171 |
| 18. | Image profile: IBM zAware partition values for the Processor page | 71 | 46. | Fields displayed in the Summary view for the current model | 173 |
| 19. | Image profile: IBM zAware partition values for the Security page. | 73 | 47. | Fields displayed in the Calendar view | 173 |
| 20. | Fields displayed on the page before the CSR is generated | 84 | 48. | Items displayed in the training calendar | 174 |
| 21. | General LDAP settings. | 85 | 49. | Fields displayed in the Ignored Messages table | 177 |
| 22. | Group LDAP settings | 86 | 50. | Fields displayed in the Add Ignored Messages window | 178 |
| 23. | Required V1R13 PTFs for z/OS monitored clients | 91 | 51. | Items displayed on the Priming Data tab | 181 |
| 24. | Fields in the Change Analysis Source window | 116 | 52. | Troubleshooting tips for the IBM zAware partition | 195 |
| 25. | Fields in the Select Nested Sort Attributes window | 124 | 53. | Troubleshooting tips for browser or GUI page displays | 195 |
| 26. | Fields displayed in the Time Line Summary window | 125 | 54. | Troubleshooting tips for running the z/OS bulk load client for IBM zAware | 197 |
| 27. | Fields displayed in the Ignore Message Status window | 126 | 55. | Troubleshooting tips for z/OS monitored clients | 197 |
| 28. | Items displayed on the SSL Settings tab | 132 | 56. | Summary of IBM zAware tasks and required IT skills, tools and information. | 205 |
| | | | 57. | IBM zAware information in the z/OS product library | 206 |
| | | | 58. | Summary of API version updates for SE-ZAWARE MCLs | 213 |

Safety

Safety notices

Safety notices may be printed throughout this guide. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs.

World trade safety information

Several countries require the safety information contained in product publications to be presented in their translation. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the translated safety information with references to the US English source. Before using a US English publication to install, operate, or service this IBM® product, you must first become familiar with the related safety information in the *Systems Safety Notices*, G229-9054. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Laser safety information

All System z® models can use I/O cards such as FICON®, Open Systems Adapter (OSA), InterSystem Channel-3 (ISC-3), or other I/O features which are fiber optic based and utilize lasers (short wavelength or long wavelength lasers).

Laser compliance

All lasers are certified in the US to conform to the requirements of DHHS 21 CFR Subchapter J for Class 1 or Class 1M laser products. Outside the US, they are certified to be in compliance with IEC 60825 as a Class 1 or Class 1M laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION: Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION: This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

About this publication

This book describes the IBM System z Advanced Workload Analysis Reporter (IBM zAware), which consists of an integrated set of applications that monitor software running on z/OS® and model normal system behavior. Its pattern recognition techniques identify unexpected messages, providing rapid diagnosis of problems caused by system changes. This early detection helps IT personnel correct problems before they affect system processing. IBM zAware is a feature of the IBM zEnterprise® EC12 (zEC12) and IBM zEnterprise BC12 (zBC12) models.

Figures included in this document illustrate concepts and are not necessarily accurate in content, appearance, or specific behavior.

Intended audience

This book is intended for experienced systems programmers and administrators who perform the following tasks:

- Configuring the logical partition (LPAR) on which IBM zAware runs.
- Preparing network and storage resources that IBM zAware requires for operation and securing access to these resources.
- Configuring z/OS operating systems to send data to IBM zAware for analysis.
- Managing the use and operation of IBM zAware, which includes controlling user access to the IBM zAware graphical user interface (GUI).
- Viewing and interpreting analytical data through the IBM zAware GUI and resolving potential problems.

Prerequisite and related information

See Appendix A, “Summary of IBM zAware tasks and required IT skills, tools and information,” on page 205, which includes references to related information in the IBM System z hardware and software product libraries.

The IBM Redbooks® publication *Extending z/OS System Management Functions with IBM zAware*, SG24-8070, documents the experiences of a team of IBMers who configured and used IBM zAware, and also describes how IBM zAware fits into the family of IBM mainframe system management tools. This Redbooks publication is available at the following URL:
<http://www.redbooks.ibm.com/>

Related HMC and SE information

The content from the following publications is now incorporated into the Hardware Management Console (HMC) and Support Element (SE) (Version 2.12.1) help system:

- *System z Hardware Management Console Operations Guide*
- *zEnterprise System Hardware Management Console Operations Guide for Ensembles*
- *zEnterprise System Support Element Operations Guide*

This information can also be found on the **System z HMC and SE (Version 2.12.1) Information Center** at <http://pic.dhe.ibm.com/infocenter/hwmca/v2r12m1/index.jsp>.

How to use this publication

This book provides an overview of IBM zAware, lists the system requirements for its infrastructure and applications, and lists the IT roles and skills required to set up and use it. This book also provides step-by-step instructions, or references to the appropriate hardware or software publications, for systems programmers and administrators who configure and manage IBM zAware or the operating systems that send data to it for analysis.

The following list describes the overall structure and content of this book:

Part 1: Introduction to IBM System z Advanced Workload Analysis Reporter (IBM zAware)

Topics in this part describe IBM zAware, explain the benefits of using it, define new terms or concepts, list hardware and software prerequisites, and provide a project plan for configuring and using IBM zAware.

Part 2: Planning to configure IBM zAware

Topics in this part explain the planning considerations that systems programmers and administrators need to know before they start configuring IBM zAware and its operating environment.

Part 3: Configuring IBM zAware and its monitored clients

Topics in this part provide instructions for configuring the IBM zAware environment, which includes the IBM zAware partition and z/OS operating systems (monitored clients) that send data for analysis. Systems programmers and administrators use these configuration tasks primarily for first-time setup.

Part 4: Managing and using IBM zAware

Topics in this part describe the IBM zAware graphical user interface (GUI) functions for daily operations, which include viewing and analyzing data from monitored clients. Additional topics include management tasks for modifying the IBM zAware configuration or operations.

Part 5: Advanced topics for managing IBM zAware

Topics in this part describe specialized management tasks for IBM zAware, such as modifying IBM zAware models of normal system behavior, planning and setting up IBM zAware for backup and recovery from failures, troubleshooting problems, and reporting problems to IBM.

Appendixes

Appendix topics include Application Programming Interfaces (APIs) that monitoring products can use to extract data from IBM zAware, and a summary of tasks and required IT skills, tools and related information in the IBM System z hardware and software product libraries.

Accessibility

This publication is in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties using this PDF file you can request a web-based format of this publication. Go to Resource Link® at <http://www.ibm.com/servers/resourcelink> and click **Feedback** from the navigation bar on the left. In the **Comments** input area, state your request, the publication title and number, choose **General comment** as the category and click **Submit**. You can also send an email to reslink@us.ibm.com providing the same information.

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.

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. Send your comments by using Resource Link at <http://www.ibm.com/servers/resourcelink>. Click **Feedback** on the navigation bar on the left. You can also send an email to reslink@us.ibm.com. Be sure to include the name of the book, the form number of the book, the version of the book, if applicable, and the specific location of the text you are commenting on (for example, a page number, table number, or a heading).

Summary of changes

For the most recent edition only, technical changes to the text are indicated by a vertical bar (|) to the left of the change.

Summary of changes for SC27-2623-01

This edition contains the following updates.

New information

- Various topics throughout this book include the new IBM zEnterprise BC12 (zBC12) as a supported IBM zAware host system.
- Chapter 2, “Prerequisites for configuring and using IBM zAware,” on page 11 lists the IBM zAware feature codes for the IBM zEnterprise BC12 (zBC12), which is a supported IBM zAware host system.
- “Estimating processor and memory resources” on page 27 contains guidelines for estimating the required amount of processor resources for IBM zAware running on a zBC12.
- “Planning network connections and capacity” on page 29 clarifies the IBM zAware requirement for an Open Systems Adapter (OSA) port for OSA-Express3 or later generation features.
- “Planning persistent storage configuration and capacity” on page 35 contains new planning considerations and best practices for configuring persistent storage for use by IBM zAware, and for backing up IBM zAware data.
- The following topics describe a new IBM zAware function through which administrators can designate specific message IDs for IBM zAware to ignore during analysis of message data from a specific monitored system. This capability is especially useful when you have recently made a change to a monitored system, such as adding a new workload.
 - “Verifying planned system changes with IBM zAware” on page 127
 - “Managing ignored messages” on page 164
 - “Manage Ignored Messages page” on page 175
- “Assigning storage devices to IBM zAware” on page 143 describes the new **Preserve data** option, which is intended for use with storage devices that contain backup copies of IBM zAware data.
- Chapter 21, “Setting up multiple IBM zAware partitions for switchover situations,” on page 187 provides instructions for configuring a primary IBM zAware server and an alternate server on the same or different host systems.
- Chapter 23, “Troubleshooting problems in the IBM zAware environment,” on page 195 provides corrective actions for problems with IBM zAware and its monitored clients.
- Appendix C, “Application Programming Interface (API) for monitoring products,” on page 213 contains new information about API versions, and descriptions of new XML fields for the LPAR and INTERVAL request types.
- Appendix D, “IBM zAware operational messages,” on page 225 contains new messages, as well as revised text and descriptions of existing messages.

Changed information

- Chapter 2, “Prerequisites for configuring and using IBM zAware,” on page 11 lists updated browser requirements for using the IBM zAware graphical user interface (GUI).
- “Matching monitored clients to a specific IBM zAware server” on page 21 contains updated information about the supported physical distance between an IBM zAware server and its monitored clients.

- “Estimating processor and memory resources” on page 27 contains updated guidelines for estimating the required amount of processor resources for IBM zAware operations. These updated guidelines are based on recent IBM test results.
- Various topics that reference the image profile for the IBM zAware partition have been updated to match the name change for the **Firmware** page; the new name is the **zAware** page. In addition, the zAware page display now provides additional information for network adapters that are defined with a Dynamic Host Connection Protocol (DHCP) type of IP address. For additional information, see Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67.
- The overview for configuring the z/OS system logger and operations log (OPERLOG) in Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91 has been reorganized and updated.
- Various topics document changes to the configuration values that determine the duration of a browser session.
 - By default, browser sessions now time out after 12 hours (720 minutes).
 - The maximum duration for a browser session is now 525600 minutes.
- Various topics contain minor technical and editorial updates.

Part 1. Introduction to the IBM System z Advanced Workload Analysis Reporter (IBM zAware)

Topics in this part describe IBM zAware, explain the benefits of using it, define new terms or concepts, list hardware and software prerequisites, and list the IT personnel and required skills for using IBM zAware.

Topics covered in this part are:

- Chapter 1, “Overview of IBM zAware,” on page 3
- Chapter 2, “Prerequisites for configuring and using IBM zAware,” on page 11
- Chapter 3, “Project plan for configuring and using IBM zAware,” on page 13

Chapter 1. Overview of IBM zAware

Today's complex, integrated data centers require a team of experts to monitor systems for abnormal behavior, and to diagnose and fix anomalies before they result in failures and outages that are visible beyond the data center. These tasks are costly and difficult for many reasons, including the fact that a variety of everyday changes can cause system anomalies. The IBM System z Advanced Workload Analysis Reporter (IBM zAware) provides a smart solution for detecting and diagnosing anomalies in z/OS systems. IBM zAware creates a model of normal system behavior based on prior system data, and uses pattern recognition techniques to identify unexpected messages in current data from the z/OS systems that it is monitoring. This analysis of events provides nearly real-time detection of anomalies that you can easily view through a graphical user interface (GUI). You also use the GUI to diagnose the cause of past or current anomalies.

Are your systems behaving badly?

Many everyday activities can introduce system anomalies and initiate failures in complex, integrated data centers; these activities include:

- Increased volume of business activity
- Application modifications to comply with changing regulatory requirements
- Standard operational changes, such as adding or upgrading hardware or software, or changing network configurations.

You can use a combination of existing system management tools to determine whether any of these activities is causing one or more systems to behave abnormally, but none can detect every possible combination of change and failure. Even when using these tools, you might have to look through message logs to help solve the problem but the sheer volume of messages can make this task a daunting one—a z/OS sysplex might produce more than 4 gigabytes (GB) of message traffic per day for its images and components alone, and application messages can significantly increase that number. More than 40000 unique message IDs are defined for z/OS and the IBM software that runs on z/OS systems.

Modernize detection and diagnosis with IBM zAware

- IBM zAware is able to analyze large quantities of message log data. Using prior message log data and mathematical modeling, IBM zAware builds a model of normal system behavior and uses it to compare to current message log data from the connected z/OS system. IBM zAware monitors the z/OS operations log (OPERLOG), which contains all messages that are written to the z/OS console, as well as suppressed messages that are not deleted after passing through any message processing controls at your installation. IBM zAware detects unusual messages and unusual message patterns that typical monitoring systems miss, as well as unique messages that might indicate system health issues. Its ability to pinpoint deviations in normal system behavior improves real-time event diagnostics.

IBM zAware automatically manages the creation of the behavioral model and manages the retention of IBM zAware analytical data for each monitored z/OS system. The number of monitored systems is limited by the data center resources that are required for collecting and storing data for monitored systems, and for IBM zAware operation.

Through the IBM zAware GUI, you can view analytical data that indicates which system is experiencing deviations in behavior, when the anomaly occurred, and whether the message was issued out of context. Using this information, you can take corrective action for these anomalies before they develop into more visible problems. Early detection and focused diagnosis can help improve time to recovery.

Finding the culprit when a problem occurs

Using the **Analysis** page in the IBM zAware GUI, you can answer key questions to diagnose a system problem. You can use either the graphical view or tabular view of the **Analysis** page to view analytical data for connected monitored clients. Figure 1 illustrates the graphical-view elements of the **Analysis** page that help you answer this question: “Which z/OS system is behaving abnormally?”

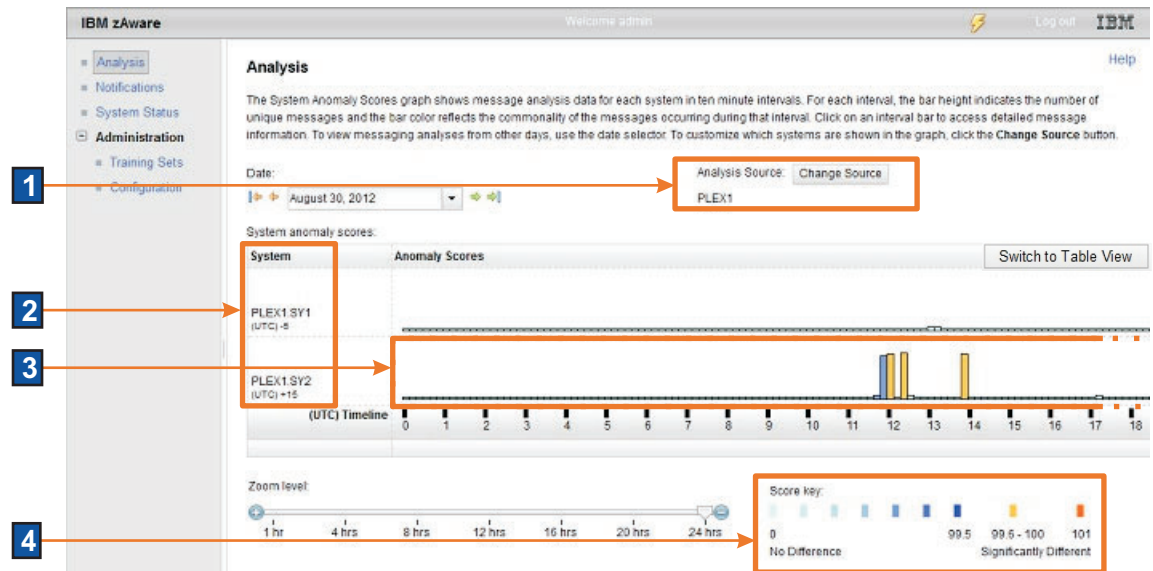


Figure 1. Elements of the **Analysis** page that help identify the problematic z/OS system

1. To begin your search, check the **Analysis Source** and adjust it as necessary. By default, all monitored systems are displayed in the **Analysis** page but you can use **Change Source** to modify the display to show systems in a specific sysplex or to show specific systems.
2. Review the names of the z/OS systems that are connected to the IBM zAware server, which are listed in the **System** column. You might need to scroll this list depending on the number of systems.
3. View the bar graphs in the **Anomaly Scores** column. Each rectangle in the graph represents a 10-minute interval; the number of unique message IDs that are issued during that interval determines the height of the rectangle.

IBM zAware uses unsupervised machine learning and IBM rules to determine interval anomaly scores:

- Through *unsupervised machine learning*, the IBM zAware server extracts and organizes message data to build a model of behavior for each monitored client. This training process is repeated over time, with the frequency determined by the training interval, which enables the server to update and refine each client model.

Through the training process, the IBM zAware server determines which messages are issued during routine system events, such as starting a batch job or a particular subsystem. For such system events, the server identifies and recognizes the pattern of messages that are associated with each event. The message patterns are called *clusters* and define the normal context for the messages in the cluster.

- z/OS experts at IBM know, based on decades of IBM experience with testing and using z/OS systems, which message IDs are likely to indicate potential problems. Message IXC101I, for example, indicates that a system is being removed from a sysplex.

Similarly, IBM experts also consider messages issued by message flood automation to be indicative of unusual behavior. Although the OPERLOG data for a monitored client might not contain all of

the messages that trigger customized automation or suppression methods in effect at your installation, IBM zAware is capable of detecting the message flood activity and marking it as anomalous.

For messages such as IXC101I and message flood automation messages, which are known to indicate potential problems, the IBM zAware server is programmed to assign high anomaly scores to the intervals in which those messages are issued.

4. Compare the color of each rectangle to the **Score key** to determine the relative anomaly score for the interval. The anomaly score indicates unusual patterns of message IDs within that interval, as compared to the model of normal system behavior. Intervals containing relatively normal, common messages receive a low score and lighter blue color, and intervals containing more unusual messages receive a higher score and darker blue or gold color. A high score indicates unusual message IDs or unusual patterns of message IDs compared to the system model.

From the interval anomaly scores shown in Figure 1 on page 4, you can determine that SY2 is a potential source of the problem because its interval anomaly scores show that many unique messages are being issued over many intervals.

Your next diagnostic question to answer is “When did this system start misbehaving?” To determine when the system began behaving abnormally, you can use various controls in the **Analysis** page to look at intervals in the past.

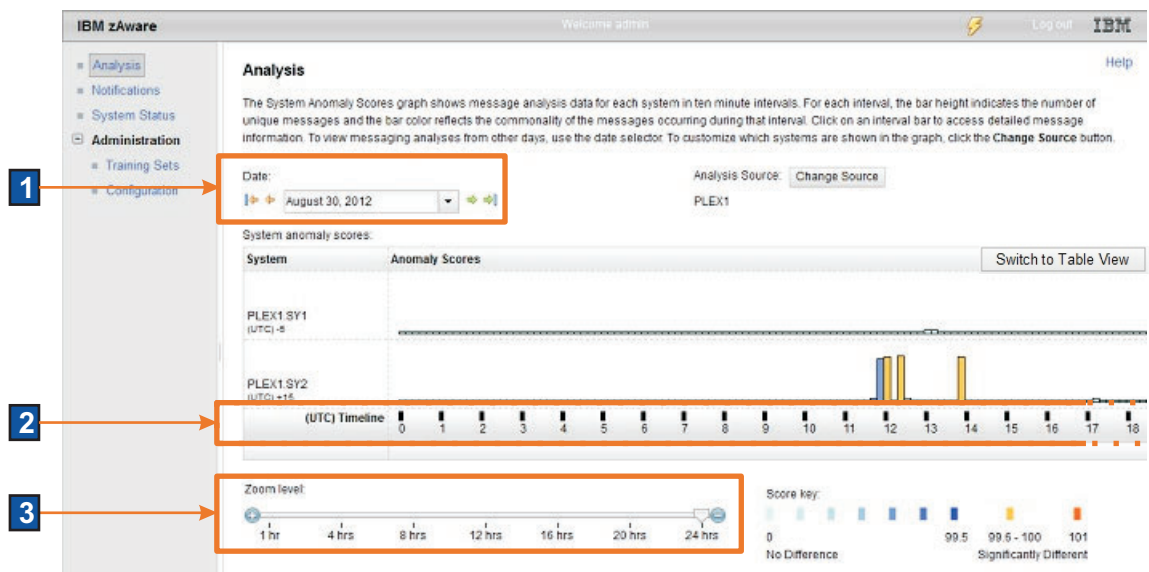


Figure 2. Elements of the **Analysis** page that change the time interval display

Figure 2 shows these controls:

1. The **Date** field displays the currently selected Coordinated Universal Time (UTC) date. You can change the current day to another date.
2. The **Timeline** marks the hours of the day in UTC, using the 24-hour clock. You can move the slider to display hours that do not show in the **Analysis** page. For a sysplex that contains systems that operate in different time zones, IBM zAware converts the times to UTC times to align the current times across monitored systems.
3. The **Zoom level** slider controls how many hours of the day are displayed in the **Analysis** page. You can move the slider to display all hours or only a few hours.

Using the **Timeline** and **Zoom level** together, you can change the display to focus on anomaly scores in a specific period.

Through these controls, you can alter the display to determine the time at which SY2 began to issue unusual messages. Hovering your cursor over the time-interval rectangle displays a summary containing the time, the number of unique message IDs issued within that time interval, and the interval anomaly score.

In summary, the **Analysis** page helps you determine which system is behaving abnormally, how many unique messages it is issuing, and when the abnormal behavior began.

To pinpoint and diagnose the problem with SY2, you might need to ask several questions:

- What message IDs are unusual?
- How often did the unusual message get issued?
- Are messages issued in context within an expected pattern?
- Is a specific z/OS component or application issuing unusual messages?
- Within the 10-minute interval, when did the message ID first appear?

To answer these diagnostic questions, use the **Interval view**, which is illustrated in Figure 3. You can display the **Interval view** for any of the 10-minute time intervals by clicking the colored rectangle in the bar graph of the **Analysis** page.

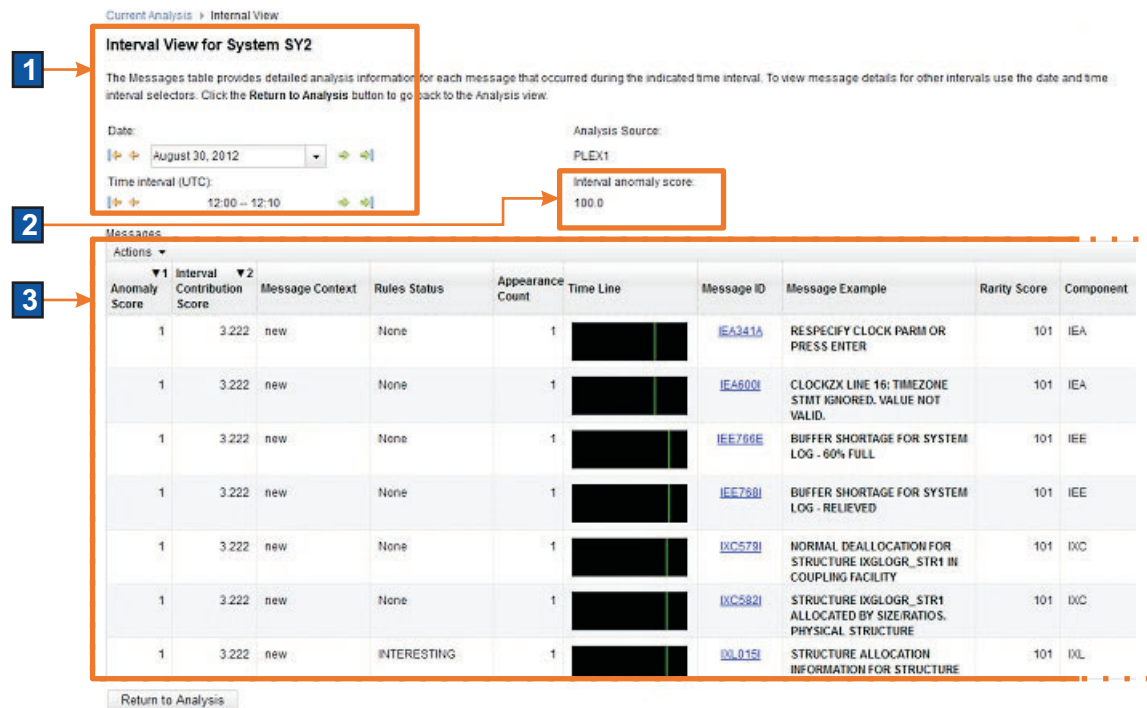


Figure 3. Elements of the **Interval view** that provide details about unique messages

The **Interval view** provides the following diagnostic details:

1. The system name, the date, and the time interval that you selected from the **Analysis** page.
2. The **Interval anomaly score**, which indicates unusual patterns of message IDs within this interval, as compared to the model of normal system behavior. This score determines the color of the rectangle that represents this interval in the bar graph on the **Analysis** page. Higher scores indicate greater anomaly so intervals with high anomaly scores are more likely to indicate a problem.
3. Details about each message issued during the interval. These details include:

Anomaly Score

Indicates the difference in expected behavior for this specific message ID within the selected interval. The message anomaly score is a combination of the interval contribution score for

this message and the rule, if any, that is in effect for this message. Higher scores indicate greater anomaly so messages with high anomaly scores are more likely to indicate a problem. The message anomaly score ranges from 0 through 1.0.

Interval Contribution Score

Indicates the relative contribution of this message to the anomaly score for the 10-minute interval. This interval score is a function of the rarity score, the number of times that the message appears within this interval, and whether the message appeared in context. Higher scores indicate greater contribution to the interval anomaly score. The interval contribution score ranges from 0 through the largest number that the Java™ double data type supports.

Message Context

Indicates whether or not this message is part of an expected pattern of messages associated with a routine system event (for example, starting a subsystem or workload). A message that is issued out of context (without the other messages in the same cluster) might indicate a problem.

Message ID

Provides the message identifier. The message ID itself is a link through which you can open a browser window, and search for an online description by using the Internet search engine of your choice.

Message Example or Message Summarization

Provides either the full message text for the first occurrence of this message within the interval, or a summary of the common message text that was issued for each occurrence of the same message.

To control the content displayed in this column, click either **View Message Full Text** or **View Message Summary** from the **Actions** list.

To increase your insight into the problem, you can sort these details by column. Select **Sort Multiple** from the **Actions** list and select the columns that you want to sort.

Monitoring behavior after a change

The **Analysis** page and **Interval view** are also useful for monitoring system behavior after you make a change to the environment, such as:

- Upgrading operating system, middleware, or application software to new levels
- Modifying system settings or configuration

In such cases, you can use the **Analysis** page and **Interval view** to determine whether any new unusual messages, or any more messages than you expected, were being issued immediately after the change.

Tracking down a random, intermittent problem

The **Analysis** page and **Interval view** are also useful for finding the cause of a random, intermittent problem. The analytical data that is available through the IBM zAware GUI can help answer the following diagnostic questions:

- Are new unusual messages issued during periods before the problem was reported, or when the problem was reported?
- Are more messages issued than expected?
- Are messages issued out of context?

Configuring the IBM zAware environment

To reap the rewards of using IBM zAware, you set up a specialized logical partition (LPAR) that is dedicated to running the IBM zAware server. This LPAR runs on a IBM zEnterprise EC12 (zEC12) central processor complex (CPC) or IBM zEnterprise BC12 (zBC12) (zBC12) CPC. Figure 4 illustrates the major elements of an IBM zAware configuration.

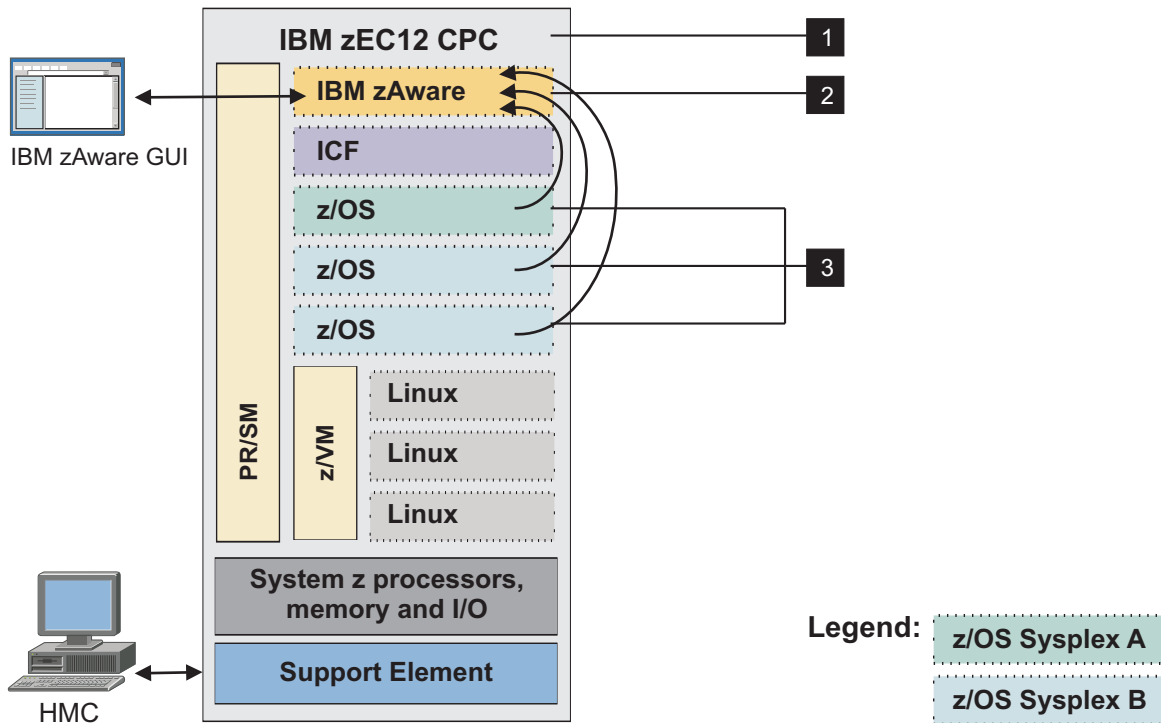


Figure 4. An IBM zAware partition running in a zEC12 CPC

1. The zEC12 CPC is called the IBM zAware *host system*. Although this figure shows a zEC12 as the host system, your installation can choose to host an IBM zAware partition on a zBC12 CPC.
2. The specialized LPAR is called the IBM zAware *partition*. An instance of IBM zAware that runs in this partition is called the IBM zAware *server*.
3. The z/OS systems that send message data to the IBM zAware server for analysis are called *monitored clients*.

The IBM zAware partition and all monitored clients that are sending information to the server running on that partition are collectively known as the IBM zAware *environment*. Monitored clients do not have to run in the same IBM zAware host system that contains the partition. Figure 5 on page 9 illustrates another possible configuration with additional z/OS monitored clients running on a IBM zEnterprise 196 (z196) CPC.

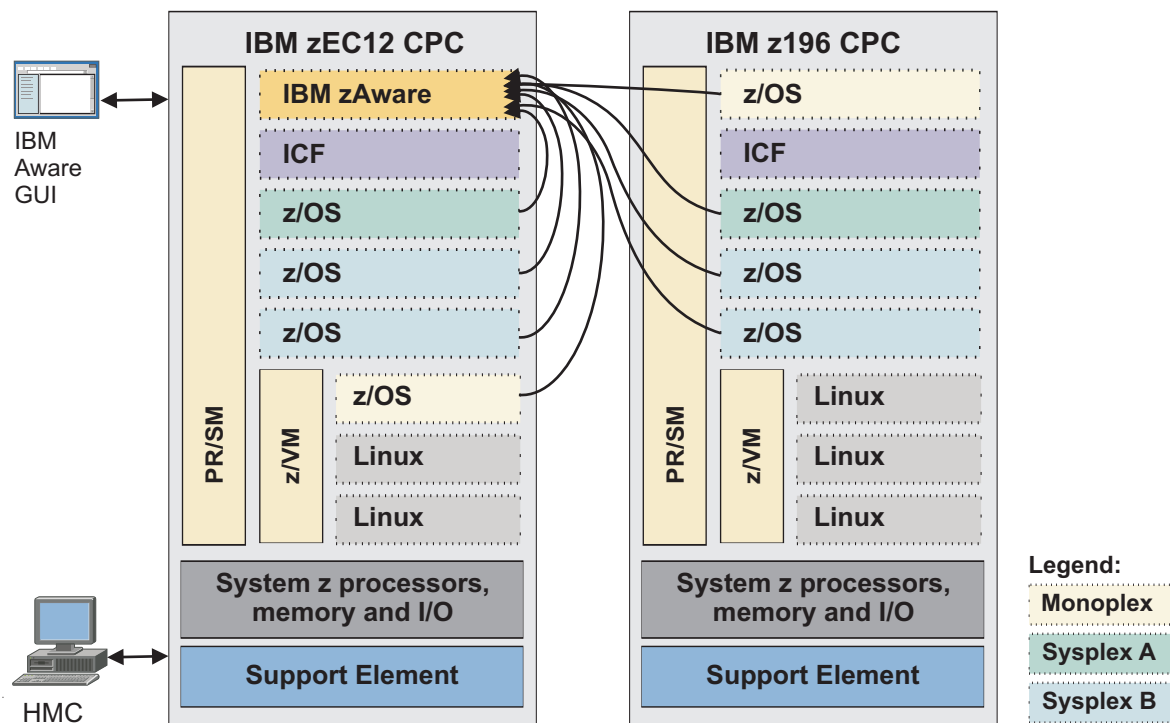


Figure 5. An IBM zAware partition supporting clients in one zEC12 CPC and one z196

In Figure 5:

- The two z/OS systems in Sysplex A (highlighted in green) are monitored clients sending data to the IBM zAware server that is running in a partition on the host system (zEC12). Only one z/OS system resides on the host system; the other z/OS system resides on the z196.
- Similarly, the four systems in Sysplex B (highlighted in blue) are all monitored clients; two reside on the host system and two reside on the z196.
- The z/OS system shown at the top of the z196 on the right is configured as a single-system sysplex (monoplex). This system is also a monitored client that is sending data to the IBM zAware server running on the host system.
- The z/OS system running as a z/VM® guest, shown on the host system, is also a monitored client that is sending data to the IBM zAware server.

Using additional IBM zAware GUI functions

In addition to providing views of analytical data for monitored clients, the IBM zAware GUI provides pages through which you can manage IBM zAware operation. Most of these tasks require the user to have administrator authority to use the GUI.

- Through **Notifications**, you can view operational messages that the IBM zAware server issues.
- Through **System Status**, you can view information about the z/OS monitored clients (systems) that are connected to the IBM zAware server.
- Through **Administration > Configuration**, you can modify default values that control the analytics engine, add or remove storage devices, manage security mechanisms, view the sysplex topology of monitored clients, and assign priming data that the IBM zAware server uses to build system behavior models.

Each model, which is called an IBM zAware model, is a description of normal behavior that is generated for a specific z/OS monitored client.

- Through **Administration > Training Sets**, you can view information about the generation of IBM zAware models, which are periodically updated by the server.

Figure 6 illustrates how system management products can use the analytical data that is presented in the IBM zAware GUI.

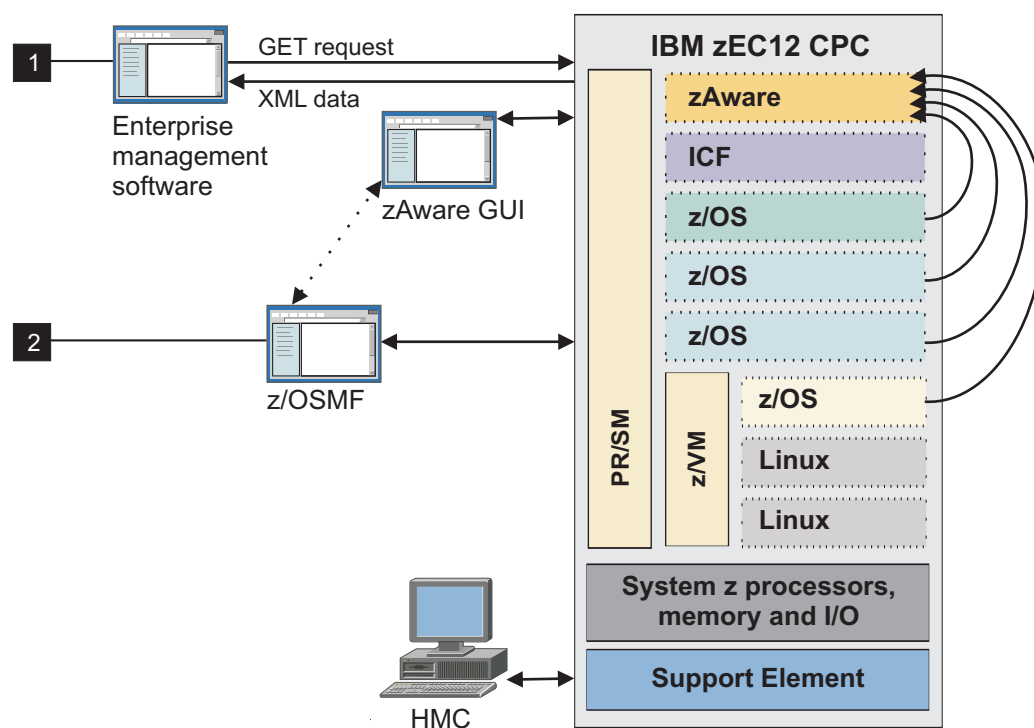


Figure 6. System management products using IBM zAware analytical data

1. Your installation can modify system management products to request and receive IBM zAware analytical data in XML format by using the IBM zAware application programming interface (API). This data is equivalent to the information that is available through the **Analysis** page and **Interval view** in the IBM zAware GUI.
2. Your installation also can configure the z/OS Management Facility (z/OSMF) so that users can launch the IBM zAware GUI from the z/OSMF **Links** page.

Chapter 2. Prerequisites for configuring and using IBM zAware

IBM zAware is available with IBM zEnterprise EC12 (zEC12) and IBM zEnterprise BC12 (zBC12) models.

Your company can order IBM zAware through the following feature codes.

Table 1. List of feature codes for ordering IBM zAware

| Model | Feature code | Description |
|----------------|--------------------------|---|
| zEC12 or zBC12 | Feature code 0011 | The IBM zAware enablement feature for a zEC12 or zBC12 that serves as the IBM zAware host system. |
| zEC12 | Feature code 0101 | IBM zAware central processor (CP) 10 pack: The feature code that represents the number of connections to IBM zAware on the zEC12 host system. |
| zEC12 | Feature code 0102 | IBM zAware disaster recovery (DR) CP 10 pack: The feature code that represents the number of connections to IBM zAware on the zEC12 that serves as a DR system. |
| zBC12 | Feature code 0138 | IBM zAware CP 2 pack |
| zBC12 | Feature code 0140 | IBM zAware CP 4 pack |
| zBC12 | Feature code 0142 | IBM zAware CP 6 pack |
| zBC12 | Feature code 0150 | IBM zAware CP 10 pack |
| zBC12 | Feature code 0139 | IBM zAware DR CP 2 pack |
| zBC12 | Feature code 0141 | IBM zAware DR CP 4 pack |
| zBC12 | Feature code 0143 | IBM zAware DR CP 6 pack |
| zBC12 | Feature code 0151 | IBM zAware DR CP 10 pack |

If you later plan to relocate or discontinue using the zEC12 or zBC12, you must remove the IBM zAware feature (0011). For instructions, see the relocation/discontinuance topic in the *zEnterprise EC12 Installation Manual*, GC28-6913 or *zEnterprise BC12 Installation Manual*, GC28-6922.

The IBM zAware partition that runs on the host or DR system requires the following resources:

- A shared or dedicated Open Systems Adapter (OSA) port, with an IP address that is either dedicated or assigned through Dynamic Host Connection Protocol (DHCP).
 - For OSA-Express3 or later generation features, IBM zAware can use only port 0.
 - With DHCP-type IP addresses, use of a domain name system (DNS) server is required.
- Shared or dedicated Integrated facilities for Linux (IFLs) or central processors (CPs).
- Storage and memory resources that are sufficient to support the IBM zAware server that runs on the partition and the z/OS clients that the server monitors.

For optimal performance and operations, configure the IBM zAware partition such that it has access to only those channel path identifiers (CHPIDs), control units, and I/O devices that are required for network connectivity and storage. For more detailed information about network connections, processors, memory, and storage for the IBM zAware partition, see Chapter 5, “Estimating data center resource requirements,” on page 27.

To become monitored clients of the IBM zAware server, z/OS systems must meet the following requirements:

- The system must be running on a supported System z server:
 - A zEC12 or zBC12
 - A IBM zEnterprise 196 (z196) or z114
 - A System z10[®] Enterprise Class (z10[™] EC) or Business Class (z10 BC)
 - Prior System z server generations, when the z/OS systems running on them can meet the operating system and configuration requirements for IBM zAware monitored clients.
- The system must be configured as a single-system sysplex (monoplex), a system in a multisystem sysplex, or a member of a Parallel Sysplex[®].
- The system must be running one of the following releases of the z/OS operating system.
 - z/OS Version 2 Release 1 (V2R1) or a later release. APAR **OA42095** is required for z/OS V2R1 only if the z/OS bulk load client is to process priming data that contains machine control characters.
 - z/OS Version 1 Release 13 (V1R13) with the following PTFs.

Table 2. Required V1R13 PTFs for z/OS monitored clients

| Component | APAR | PTF |
|--|---|--|
| BCP system logger | APAR OA38747 | PTF UA66494 HBB7780 PTF UA66495 JBB778J |
| BCP system logger | APAR OA38613 Prerequisite for APAR OA38747 | PTF UA66195 HBB7780 PTF UA66196 JBB778J |
| BCP z/OS bulk load client for IBM zAware | APAR OA39256 APAR OA42095 ¹ | PTF UA66522 HBB7780 PTF UA69292 HBB7780 PTF UA69293 HBB7780 |
| Footnote: | | |
| 1. APAR OA42095 is required for z/OS V1R13 only if the z/OS bulk load client is to process priming data that contains machine control characters. | | |

- The system must be using the operations log (OPERLOG) as the hardcopy medium.
- The system name and sysplex name must uniquely identify the system to be monitored. IBM zAware identifies each monitored client by sysplex and system name, in the format *sysplex_name.system_name*; for example: SYSPLEX1.SYSA. IBM zAware cannot monitor more than one system with the same sysplex and system name combination.

To take full advantage of the IBM zAware graphical user interface (GUI), you must use one of the following browsers. Edit your browser options to enable JavaScript, Cascading Style Sheets (CSS) and cookies, and to disable software that blocks pop-up windows, especially if you are using keyboard controls rather than the mouse to use the GUI.

- Mozilla Firefox Extended Support Release (ESR) 17
- Microsoft Windows Internet Explorer 9, with compatibility mode disabled

Other browsers and browser release levels might work but have not been tested; if you use them, some IBM zAware functions might not be available and page content might not display correctly.

For the most recent hardware planning and corequisite software information, go to IBM Resource Link: <http://www.ibm.com/servers/resourceLink>

- For hardware updates, click **Tools** on the navigation panel. Then click **Machine information** under **Servers**, and enter your enterprise number, customer number, or machine serial number for the zEC12 or zBC12. You must register with IBM to search machine information.
- For software updates, click **Fixes** on the navigation panel. Then click **Preventative Service Planning buckets (PSP)** under **Preventive actions**, and check the 2827DEVICE PSP bucket for the zEC12 or the 2828DEVICE PSP bucket for the zBC12.

Chapter 3. Project plan for configuring and using IBM zAware

System planners and installation managers collaborate with specialized IT personnel to plan, configure, and manage IBM zAware. The following checklists provide a task summary, identify the IT role or skill required for each task, and provide links to further details.

Phase 1: Planning

The planning phase includes identifying the IBM zAware host system and z/OS monitored clients, and determining datacenter resources required for IBM zAware server operation.

Table 3. Planning checklist for the IBM zAware environment

| ✓ | Task summary: | IT role / skills: | Where to find instructions: |
|---|--|---|---|
| | Plan the configuration of the IBM zAware environment. | System planners and installation managers | Chapter 4, "Planning your IBM zAware environment," on page 19 |
| | Plan the LPAR characteristics of the IBM zAware partition. | System planner | "Estimating processor and memory resources" on page 27 |
| | Plan the network connections required for the IBM zAware partition and each z/OS monitored client. | Network administrator | "Planning network connections and capacity" on page 29 |
| | Plan the physical storage capacity required to support the IBM zAware server and its monitored clients. | Storage administrator | "Planning persistent storage configuration and capacity" on page 35 |
| | Plan the security requirements for the IBM zAware server, its monitored clients, and users of the IBM zAware graphical user interface (GUI). | Security administrator | Chapter 6, "Planning for security," on page 51 |
| | Plan for using the IBM zAware GUI | System planner | Chapter 7, "Planning to use the IBM zAware GUI," on page 55 |
| | Plan to create initial IBM zAware models for monitored clients | System programmer | Chapter 8, "Planning to create IBM zAware models," on page 57 |

Phase 2: Configuring the IBM zAware partition

This configuration phase encompasses first-time setup tasks for the IBM zAware partition.

Table 4. Configuration checklist for the IBM zAware partition

| ✓ | Task summary: | IT role / skills: | Where to find instructions: |
|---|--|-----------------------|--|
| | Verify that your installation meets the prerequisites for using IBM zAware | System programmer | Chapter 2, "Prerequisites for configuring and using IBM zAware," on page 11 |
| | Configure network connections for the IBM zAware partition through the Hardware Configuration Definition (HCD) or the Input/Output Configuration Program (IOCP). | Network administrator | Step 1 on page 64 in Chapter 9, "Configuring network connections and storage for the IBM zAware partition," on page 63 |
| | Configure persistent storage for the IBM zAware partition through the HCD or IOCP. | Storage administrator | Step 2 on page 65 in Chapter 9, "Configuring network connections and storage for the IBM zAware partition," on page 63 |

Table 4. Configuration checklist for the IBM zAware partition (continued)

| ✓ | Task summary: | IT role / skills: | Where to find instructions: |
|---|--|-----------------------|---|
| | Define the LPAR characteristics of the IBM zAware partition through the Hardware Management Console (HMC). | System programmer | Chapter 10, "Configuring an image profile for the IBM zAware partition," on page 67 |
| | Define network settings for the IBM zAware partition through the HMC. | Network administrator | Step 7 on page 75 in Chapter 10, "Configuring an image profile for the IBM zAware partition," on page 67. |
| | Activate the IBM zAware partition through the HMC. | System programmer | Follow the operating procedures at your company for activating a partition on a zEC12 CPC. |

Phase 3: Configuring the IBM zAware server and its monitored clients

This configuration phase encompasses first-time setup tasks for the IBM zAware server and its z/OS monitored clients.

Table 5. Configuration checklist for the IBM zAware server and monitored clients

| ✓ | Task summary: | IT role / skills: | Where to find instructions: |
|---|---|--|---|
| | Assign storage devices for the IBM zAware server through the IBM zAware GUI. | Storage administrator | Step 2 on page 81 in Chapter 11, "Configuring storage, security, and analytics for the IBM zAware server," on page 79 |
| | Optional: Replace the default Secure Sockets Layer (SSL) certificate that is configured in the IBM zAware server. | Security administrator | Step 3 on page 83 in Chapter 11, "Configuring storage, security, and analytics for the IBM zAware server," on page 79 |
| | Configure an LDAP repository or local file-based repository for authenticating users of the IBM zAware GUI. | Security administrator or LDAP administrator | <ul style="list-style-type: none"> To configure an LDAP repository, see step 4 on page 84 in Chapter 11, "Configuring storage, security, and analytics for the IBM zAware server," on page 79. To configure a file-based repository, see Chapter 20, "Setting up a local repository to secure access to the IBM zAware GUI," on page 185. |
| | Authorize users or groups to access the IBM zAware GUI. | Security administrator | Step 5 on page 87 in Chapter 11, "Configuring storage, security, and analytics for the IBM zAware server," on page 79 |
| | Modify the configuration values that control IBM zAware analytics operation. | System programmer | Step 8 on page 88 in Chapter 11, "Configuring storage, security, and analytics for the IBM zAware server," on page 79 |
| | Configure a network connection for each z/OS monitored client through the TCP/IP profile. If necessary, update firewall settings. | Network administrator | Step 1 on page 92 in Chapter 12, "Configuring z/OS monitored clients to send data to the IBM zAware server," on page 91. |
| | Verify that each z/OS system meets the sysplex configuration and OPERLOG requirements for IBM zAware monitored clients. | z/OS system programmer | Steps 2 on page 93 and 6 on page 95 in Chapter 12, "Configuring z/OS monitored clients to send data to the IBM zAware server," on page 91 |
| | Configure the z/OS system logger to send data to the IBM zAware server. | z/OS system programmer | Steps 3 on page 93 to 7 on page 96 in Chapter 12, "Configuring z/OS monitored clients to send data to the IBM zAware server," on page 91 |

Table 5. Configuration checklist for the IBM zAware server and monitored clients (continued)

| ✓ | Task summary: | IT role / skills: | Where to find instructions: |
|---|--|------------------------|--|
| | Prime the IBM zAware server with prior data from monitored clients. | z/OS system programmer | Steps 1 on page 101 and 2 on page 103 in Chapter 13, "Creating an IBM zAware model for new z/OS monitored clients," on page 99 |
| | Build a model of normal system behavior for each monitored client. The IBM zAware server uses these models for analysis. | z/OS system programmer | Steps 3 on page 103 to 5 on page 105 in Chapter 13, "Creating an IBM zAware model for new z/OS monitored clients," on page 99 |

Phase 4: Daily operations

In this phase, the primary activity is viewing IBM zAware analytical data to find and diagnose anomalies in the behavior of z/OS monitored clients. z/OS system programmers and experienced application programmers are the most likely IT personnel to participate in this activity. Topics in the following parts describe this ongoing activity and other occasional management tasks.

- Part 4, "Managing and using the IBM zAware server," on page 107
- Part 5, "Advanced topics for managing IBM zAware," on page 157

Part 2. Planning to configure IBM zAware

Topics in this part explain the planning considerations that system planners, installation managers and network, storage and security administrators need to know before they start configuring IBM zAware and its operating environment.

Topics covered in this part are:

- Chapter 4, “Planning your IBM zAware environment,” on page 19
- Chapter 5, “Estimating data center resource requirements,” on page 27
- Chapter 6, “Planning for security,” on page 51
- Chapter 7, “Planning to use the IBM zAware GUI,” on page 55
- Chapter 8, “Planning to create IBM zAware models,” on page 57

Chapter 4. Planning your IBM zAware environment

The IBM zAware environment consists of an IBM zAware partition, the IBM zAware server running on that partition, and all of the monitored clients that are connected to the server. This topic provides illustrations of sample configurations for the IBM zAware environment, and introduces planning considerations that are covered in more detail in other planning chapters.

Supported types of System z servers

- | The IBM zAware partition runs on a zEC12 central processor complex (CPC) or zBC12 CPC, so every supported configuration must include a zEC12 or zBC12 host system. The IBM zAware partition that runs on the host system requires the following resources:
 - A shared or dedicated Open Systems Adapter (OSA) port, with an IP address that is either dedicated or assigned through Dynamic Host Connection Protocol (DHCP).
 - | – For OSA-Express3 or later generation features, IBM zAware can use only port 0.
 - | – With DHCP-type IP addresses, use of a domain name system (DNS) server is required.
 - Shared or dedicated Integrated facilities for Linux (IFLs) or central processors (CPs).
 - Storage and memory resources that are sufficient to support the IBM zAware server that runs on the partition and the z/OS clients that the server monitors.

Chapter 5, “Estimating data center resource requirements,” on page 27 provides more detail about these resource requirements.

- | Monitored clients can run in partitions on the zEC12 or zBC12 host system or in partitions on the following System z servers:
 - A IBM zEnterprise 196 (z196) or z114
 - A System z10 Enterprise Class (z10 EC) or Business Class (z10 BC)
 - Prior System z server generations, when the z/OS systems running on them can meet the operating system and configuration requirements for IBM zAware monitored clients.

Supported types of IBM zAware monitored clients

IBM zAware supports z/OS systems that run in z/OS partitions or as z/VM guests. The number of clients is limited only by the resources assigned to the IBM zAware partition. z/OS monitored clients must meet the following requirements:

- The system must be configured as a single-system sysplex (monoplex), a system in a multisystem sysplex, or a member of a Parallel Sysplex.
- The system must be running one of the following releases of the z/OS operating system.
 - | – z/OS Version 2 Release 1 (V2R1) or a later release. APAR **OA42095** is required for z/OS V2R1 only if the z/OS bulk load client is to process priming data that contains machine control characters.
 - | – z/OS Version 1 Release 13 (V1R13) with the following PTFs.

Table 6. Required V1R13 PTFs for z/OS monitored clients

| Component | APAR | PTF |
|-------------------|---|--|
| BCP system logger | APAR OA38747 | PTF UA66494 HBB7780 PTF UA66495 JBB778J |
| BCP system logger | APAR OA38613 Prerequisite for APAR OA38747 | PTF UA66195 HBB7780 PTF UA66196 JBB778J |

Table 6. Required V1R13 PTFs for z/OS monitored clients (continued)

| Component | APAR | PTF |
|---|---------------------------|---------------------|
| BCP z/OS bulk load client for IBM zAware | APAR OA39256 | PTF UA66522 HBB7780 |
| | APAR OA42095 ¹ | PTF UA69292 HBB7780 |
| | | PTF UA69293 HBB7780 |
| Footnote: 1. APAR OA42095 is required for z/OS V1R13 only if the z/OS bulk load client is to process priming data that contains machine control characters. | | |

- The system must be using the operations log (OPERLOG) as the hardcopy medium.
- The system name and sysplex name must uniquely identify the system to be monitored. IBM zAware identifies each monitored client by sysplex and system name, in the format *sysplex_name.system_name*; for example: SYSPLEX1.SYSA. IBM zAware cannot monitor more than one system with the same sysplex and system name combination.

Figure 7 illustrates all of the supported types of z/OS monitored clients. They are all running on a zEC12 but the zEC12 on the right could be another supported type of System z server.

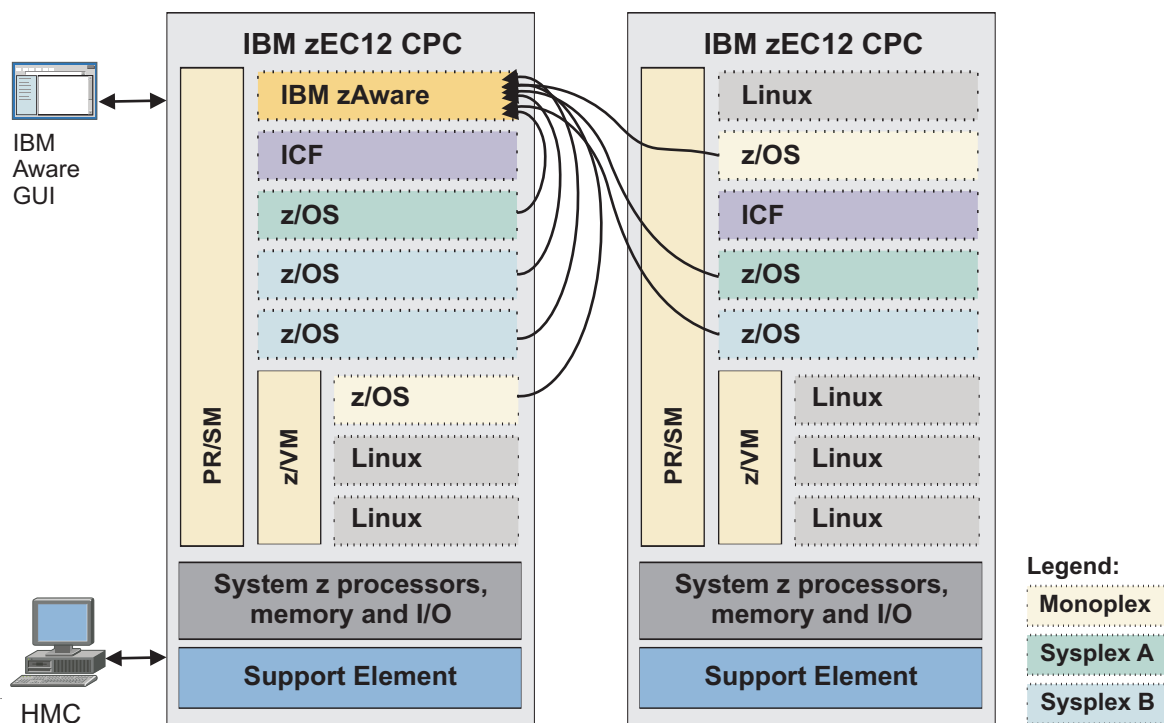


Figure 7. Types of z/OS monitored clients connected to a IBM zAware partition in a zEC12 CPC

The IBM zAware environment in Figure 7 contains one IBM zAware, the server that runs on the partition, and monitored clients that run on the zEC12 (the IBM zAware host system). Additional clients run in partitions on another zEC12; clients that run on a System z server other than the host system are called *remote clients*.

- The host system contains partitions in which the following monitored clients run:
 - One z/OS system in Sysplex A (highlighted in green)
 - Two systems in Sysplex B (highlighted in blue)
 - One z/OS system, which is configured as a single-system sysplex (monoplex), running as a z/VM guest
- The zEC12 on the right contains the remote clients:

- One z/OS system, configured as a single-system sysplex (monoplex)
- Another z/OS system in Sysplex A (highlighted in green)
- Another system in Sysplex B (highlighted in blue)

In addition to the previously listed system prerequisites, the workload type and message traffic determine which z/OS systems are candidates for monitoring through IBM zAware. Systems that run production workloads are obvious choices because of their importance to your business, and your reliance on their availability. Production systems also tend to have high-volume, consistent message traffic that IBM zAware can use to build a useful model of normal system behavior. Chapter 8, “Planning to create IBM zAware models,” on page 57 describes the specific attributes of message traffic that are required to create an IBM zAware model.

Quality assurance (QA) systems are also well-suited for monitoring through IBM zAware. Test and development systems, on the other hand, might not warrant configuration as monitored clients. Because of their inherent unpredictability, you might find it difficult to generate a model of normal system behavior that yields useful analytical data.

Matching monitored clients to a specific IBM zAware server

- | The physical distance between an IBM zAware server and its monitored clients can determine the configuration of your IBM zAware environment. IBM testing experiences indicate acceptable IBM zAware capability and performance up to a maximum distance of 3500 kilometers (approximately 2174 miles) between the zEC12 or zBC12 host system and monitored clients that run on other System z servers.
- | Figure 8 on page 22 illustrates an IBM zAware configuration that requires two separate servers because of the distance between the two company sites. For this example, the company configures two IBM zAware partitions to monitor the production systems that are running on four zEC12 servers:
- | • In the zEC12 host on the upper left of the figure, the IBM zAware server monitors clients that reside on the host and on two other zEC12 servers at the Boston site. These clients are members of either Sysplex A (highlighted in green) or Sysplex B (highlighted in blue).
- | • In the zEC12 host on the lower left of the figure, another IBM zAware server monitors clients that reside on the host at the Los Angeles site. These clients are all members of Sysplex C (highlighted in dark blue).

Notice that each site illustrated in Figure 8 on page 22 has its own firewall, and that each IBM zAware environment— the server and all of its monitored clients— are protected by that firewall. Because IBM zAware does not provide any encryption or authentication for communication from monitored clients, the recommended configuration is to protect the IBM zAware and its clients with the same firewall.

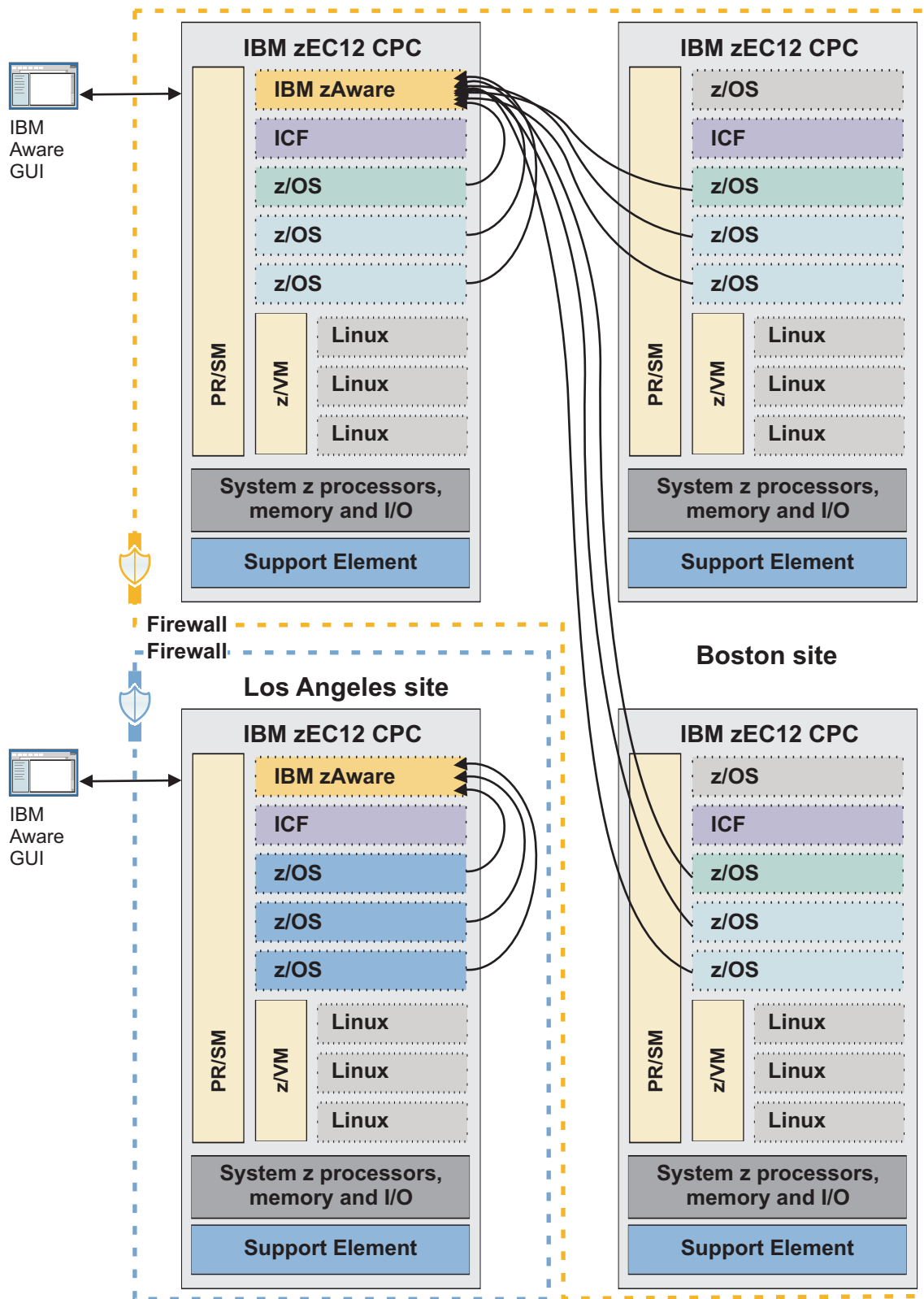


Figure 8. An IBM zAware configuration with two partitions, each supporting the clients in one of two physical sites

Figure 9 illustrates another possible configuration with two IBM zAware partitions. Because the zEC12 has multiple firewalls, the company configured each IBM zAware server and its clients to be protected by the same firewall.

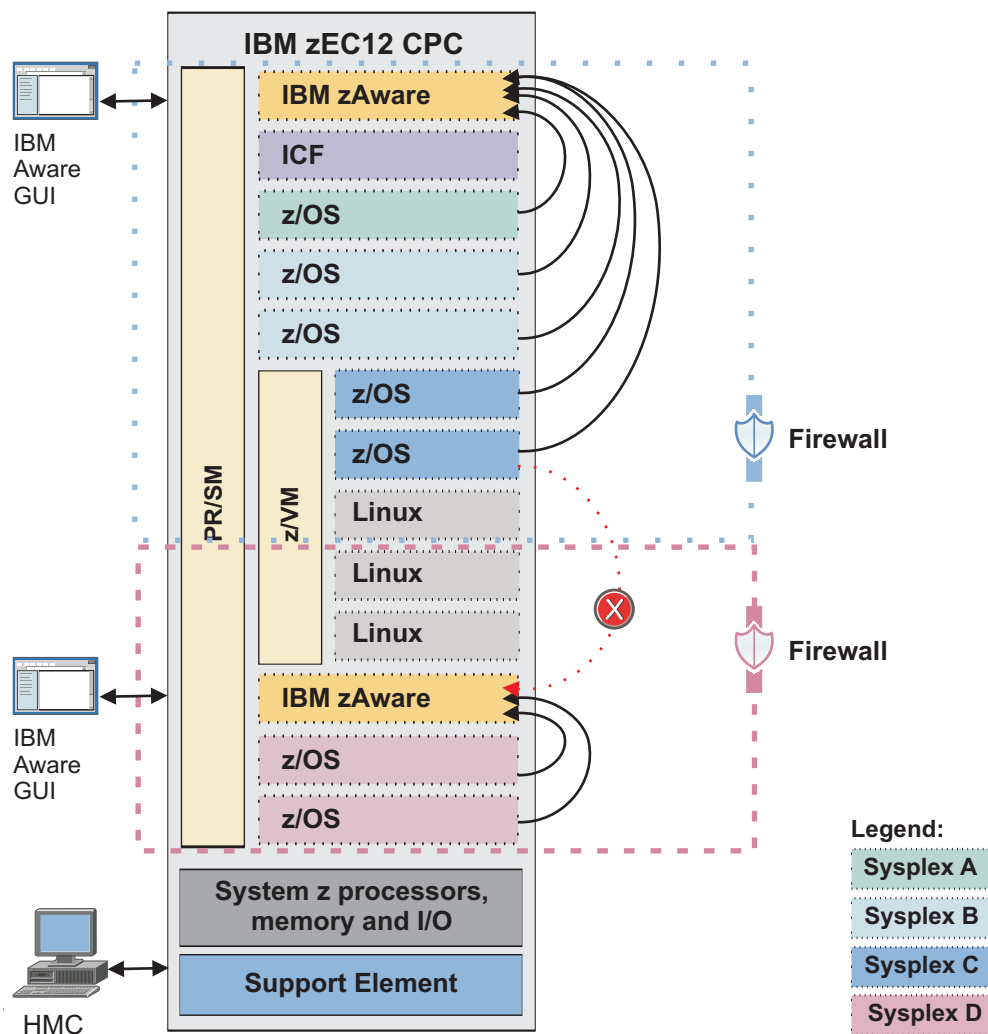


Figure 9. Two IBM zAware partitions in one zEC12 CPC with multiple firewalls

In Figure 9 on page 23:

- All clients protected by the upper firewall (highlighted in blue) are connected to the IBM zAware server running in the partition protected by the upper firewall. The clients are members of Sysplex A, Sysplex B, or Sysplex C.
- All clients protected by the lower firewall (highlighted in pink) are connected to the IBM zAware server running in the partition protected by the lower firewall. The clients are members of Sysplex D.
- The dotted red line from one Sysplex C client illustrates two possible configurations that are **not** recommended:
 - Configuring a monitored client to connect to an IBM zAware server that is protected by a different firewall.

IBM zAware does not require clients to provide authentication credentials or to encrypt the operations log (OPERLOG) data that they send. If your installation considers this data to be sensitive, you need to ensure that the communication between IBM zAware and its monitored clients occurs over secured networks that are configured with preexisting security mechanisms. One method of ensuring secure communication between the server and its clients is to configure them so that they are protected by the same firewall. Additional network and security considerations are covered in the following topics:

- “Planning network connections and capacity” on page 29
- “Securing communication between IBM zAware and its monitored clients” on page 51
- Using different IBM zAware servers to monitor clients that belong to the same sysplex.

You can choose to configure only some members of the same sysplex as monitored clients; not all members of a sysplex have to be connected to the IBM zAware server. In some cases, all sysplex members cannot be connected; for example, in a Geographically Dispersed Parallel Sysplex™ (GDPS®), the controlling system (K-system) cannot be a monitored client because you cannot use OPERLOG on a K-system. However, any members of the same multiple-system sysplex that you do configure as monitored clients must be clients of the same IBM zAware server.

Figure 10 on page 25 illustrates a more complex configuration that contains all types of supported monitored clients. These clients run in partitions on different types of System z servers that are protected by the same firewall, even though they are physically separated in two different buildings at the company's Boston site.

- All monitored clients are connected to the IBM zAware server running in the partition on the zEC12 host system.
- The z/OS system shown at the top of the z114 on the upper right is configured as a single-system sysplex (monoplex). This system is also a monitored client that is sending data to the IBM zAware server.
- Each member of Sysplex A (highlighted in green) runs on a different System z server; all members are connected and sending data to the IBM zAware server.
- Similarly, the members of Sysplex B (highlighted in blue) and Sysplex C (highlighted in dark blue) run on different System z servers, and all members are connected and sending data to the IBM zAware server.
- The members of Sysplex D (highlighted in pink) run as z/VM guests on the z196; all are connected and sending data to the IBM zAware server.

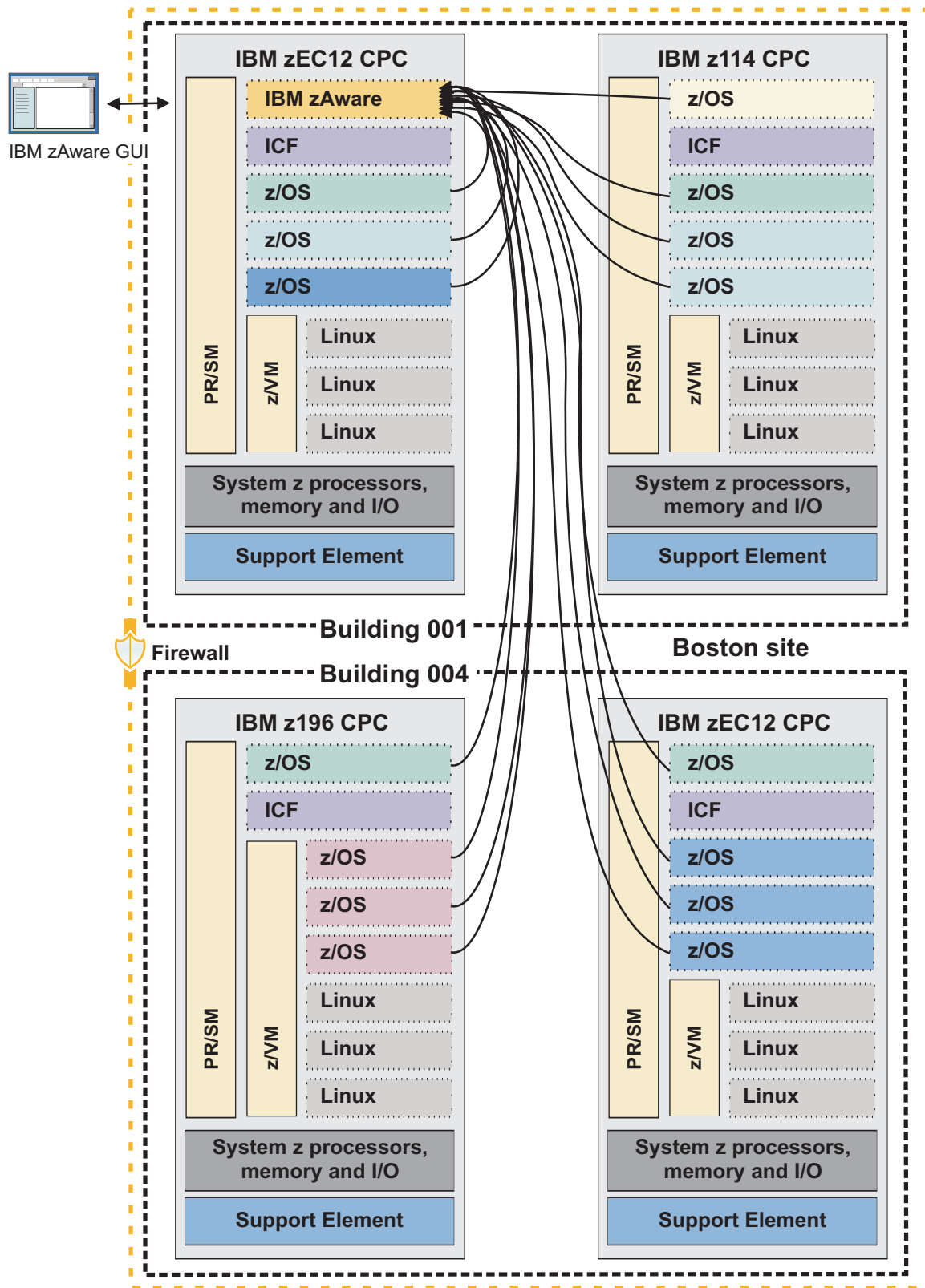


Figure 10. An IBM zAware environment containing sysplexes that are split between two physical buildings

Summary of planning considerations for the IBM zAware environment

- | • The IBM zAware partition runs on a zEC12 or zBC12 host system and requires specific data center resources. Chapter 5, “Estimating data center resource requirements,” on page 27 provides more information about these requirements.
- z/OS monitored clients must meet specific configuration requirements and exhibit specific message traffic attributes so the IBM zAware server can build a useful model of system behavior. Production systems and QA systems generally meet these message traffic requirements.
 - Chapter 8, “Planning to create IBM zAware models,” on page 57 provides more information about message traffic attributes.
 - Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91 provides an overview of configuration requirements.
- The recommended configuration for an IBM zAware environment— the partition, the server, and its monitored clients— is to protect them with the same firewall.
- | • The physical distance between an IBM zAware server and its monitored clients can determine the
| configuration of your IBM zAware environment. IBM testing experiences indicate acceptable IBM
| zAware capability and performance up to a maximum distance of 3500 kilometers (approximately 2174
| miles) between the zEC12 or zBC12 host system and monitored clients that run on other System z
| servers.
- Members of the same multiple-system sysplex must be connected to the same IBM zAware server.

Chapter 5. Estimating data center resource requirements

The processor, memory, network and storage resources that IBM zAware requires vary by installation. The following topics provide guidelines for determining these resource requirements.

- “Estimating processor and memory resources”
- “Planning network connections and capacity” on page 29
- “Planning persistent storage configuration and capacity” on page 35

Estimating processor and memory resources

| According to IBM test results, the amount of required processing resource for the IBM zAware partition
| varies depending on the number of monitored clients and their combined total rate of message traffic,
| and also on the phase of IBM zAware operation. Use the guidelines in this topic to determine the amount
| of processor and memory resource that your installation requires.

Determining the rate of message traffic for a z/OS system

| To determine the rate of message traffic for the purposes of estimating processor resource requirements,
| you can use one of the following options. With either option, the key metric is the total number of
| message lines, rather than the number of unique message identifiers (IDs).

- IBM message analysis program

Using the IBM message analysis program is perhaps the easiest way to analyze the message traffic for a given z/OS monitored client. Through this program, you can analyze z/OS SYSLOG data sets to determine the message rate per second, as well as the number and frequency of unique message IDs. The message analysis program is available on the z/OS Tools and Toys web site at the following URL:
<http://www-03.ibm.com/systems/z/os/zos/features/unix/bpxalty2.html>

To find the message analysis program, search the table of download packages for the MSGLG610 package.

- Manual calculation

| As an alternative to using the message analysis program, you can calculate the maximum message rate
| by completing the following steps:

- | 1. Select a peak workload interval for the z/OS system and store the OPERLOG messages for that
| interval.
- | 2. Choose a precise 10-minute interval from the stored messages, and count the messages issued
| during that interval. For any multiline messages that might have been issued during the interval,
| count each line.
- | 3. Divide the message count by 600 to obtain the message rate per second.

Calculating processor and memory resources

The following guidelines are based on IBM testing of the two operations phases:

- The initial priming and training phase for the IBM zAware server, during which your installation:
 - Uses the z/OS bulk load client for IBM zAware to transfer prior data for monitored clients.
 - Requests the server to build a model for each client from the transferred data.
- Normal operations, during which the primary IBM zAware activity is the analysis of current data from monitored clients.

Processor resources

On either a zEC12 or zBC12, your installation can assign only one of two processor types for the IBM zAware partition: Integrated facilities for Linux (IFLs) or central processors (CPs). The IFLs or CPs can be shared or dedicated.

Use the following guidelines to determine the amount of processor resource that your installation requires. Keep in mind that IFLs run at full capacity, but CPs can run at full capacity or various subcapacity settings, depending on the zEC12 or zBC12 model. These guidelines are based on IFLs or CPs that are running at full capacity.

For an IBM zAware partition on a zEC12

- For configurations with up to 10 monitored clients, for a total maximum rate of 500 messages per second:
 - Approximately 25% of one zEC12 IFL or 25% of one full-capacity zEC12 CP (for example, model 701) is required for initial priming and training.
 - Approximately 20% of one zEC12 IFL or 20% of one full-capacity zEC12 CP (for example, model 701) is required for analysis operations.
- For configurations with up to 10 monitored clients, for a total maximum rate of 1500 messages per second:
 - Approximately 80% of one zEC12 IFL or 80% of one full-capacity zEC12 CP (for example, model 701) is required for initial priming and training.
 - Approximately 40% of one zEC12 IFL or 40% of one full-capacity zEC12 CP (for example, model 701) is required for analysis operations.

If you connect more than 10 monitored images during a 15-minute interval when the maximum message rate per second is approximately 1500, the capacity of a single zEC12 IFL or a single full-capacity zEC12 CP might be overrun during the initial priming and training phase. To avoid this potential condition, you can configure a second zEC12 IFL or CP for IBM zAware to use.

For an IBM zAware partition on a zBC12

- For configurations with up to 10 monitored clients, for a total maximum rate of 500 messages per second:
 - Approximately 30% of one zBC12 IFL or 30% of one full-capacity zBC12 CP (for example, model z01) is required for initial priming and training.
 - Approximately 20% of one zBC12 IFL or 20% of one full-capacity zBC12 CP (for example, model z01) is required for analysis operations.
- For configurations with up to 10 monitored clients, for a total maximum rate of 1500 messages per second:
 - Approximately 95% of one zBC12 IFL or 95% of one full-capacity zBC12 CP (for example, model z01) is required for initial priming and training.
 - Approximately 40% of one zBC12 IFL or 40% of one full-capacity zBC12 CP (for example, model z01) is required for analysis operations.

If you connect more than 10 monitored images during a 15-minute interval when the maximum message rate per second is approximately 1500, the capacity of a single zBC12 IFL or CP might be overrun during the initial priming and training phase. To avoid this potential condition, you can configure a second zBC12 IFL or CP for IBM zAware to use.

Memory

Use the following guidelines to determine the amount of memory that an IBM zAware partition requires for your installation. These guidelines apply for an IBM zAware partition on either a zEC12 or a zBC12.

- You must allocate a minimum of 4096 MB (4 GB) to activate the IBM zAware partition. This amount of memory is sufficient to support a relatively small number of monitored clients (six or fewer) with relatively light message traffic (500 messages per second).

- If your installation plans to connect more than six monitored clients, you need to assign an additional 256 MB of memory for each monitored client. Use the following formula for determining the amount of memory to assign to the partition.

$$4096\text{MB} + (256\text{MB} * (\text{number of clients}))$$

See the following topics for additional information:

- Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67 contains instructions for specifying processor and memory requirements in the image profile for the partition.
- “Monitoring processor and memory resources” on page 154 contains information about monitoring and adjusting these resources.

Planning network connections and capacity

After you decide which z/OS systems to monitor with IBM zAware, you need to plan the network connections that are required to enable communication between the IBM zAware server and its clients. Your choices are dependent on the types of network connections that the IBM zAware server supports and on the location of the monitored clients.

The IBM zAware server requires a shared or dedicated Open Systems Adapter (OSA) port and an IP address for the partition in which the server runs.

- For OSA-Express3 or later generation features, IBM zAware can use only port 0.
- The IP address must be either dedicated or assigned through Dynamic Host Connection Protocol (DHCP). With DHCP-type IP addresses, use of a domain name system (DNS) server is required.

The server supports the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

The IBM zAware server supports the following types of network options, which are shown in a simple configuration in Figure 11 on page 30.

- A customer-provided data network that provides Ethernet connectivity through an OSA channel.
- A HiperSockets™ subnet within the zEC12 CPC.

HiperSockets is a hardware feature that provides high performance internal communications between logical partitions within the same CPC, without the use of any additional or external hardware equipment.

- The intraensemble data network (IEDN) on the zEC12 CPC.

The IEDN is a private high-speed network for application data communications within and between nodes of an ensemble. The IBM zAware server also supports the use of HiperSockets over the IEDN.

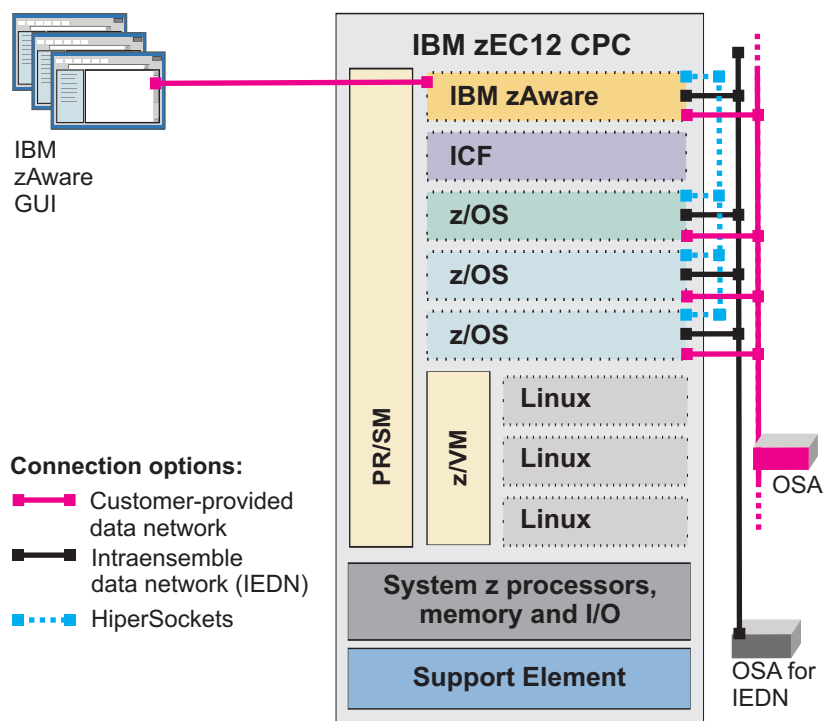


Figure 11. Supported network connection options for the IBM zAware environment

The simple configuration in Figure 11 shows the IBM zAware server and all of its monitored clients residing on the same zEC12 CPC. For this type of configuration, you need to configure the following network connections:

- An OSA channel path for browser access to the IBM zAware server. Of the supported network options, the OSA channel is the most logical choice for allowing browser connections to the server, so users can view the analytical data for the monitored clients through the IBM zAware graphical user interface (GUI).
- Any one of the supported network options for connecting an IBM zAware server to z/OS monitored clients: an OSA channel, HiperSockets subnet, or the IEDN. In this case, factors other than the location of z/OS clients might influence your choice. For example, you might need to consider security mechanisms or the possible impact to current network traffic of additional message traffic from the z/OS clients to the server.

If you expand the IBM zAware environment to include z/OS systems that reside on other CPCs at your installation, your options are different. For example, suppose that you want to monitor z/OS clients that belong to two sysplexes, A and B, which have some system images on the zEC12 CPC and others on an IBM System z10 CPC, as shown in Figure 12 on page 31. For the clients on the z10 CPC, your only option is an OSA channel because the System z10 CPC cannot use the IEDN and HiperSockets provide an internal network channel only within a single CPC. Depending on the complexity of the IBM zAware environment that you plan to configure, you might define all three types of supported network connections.

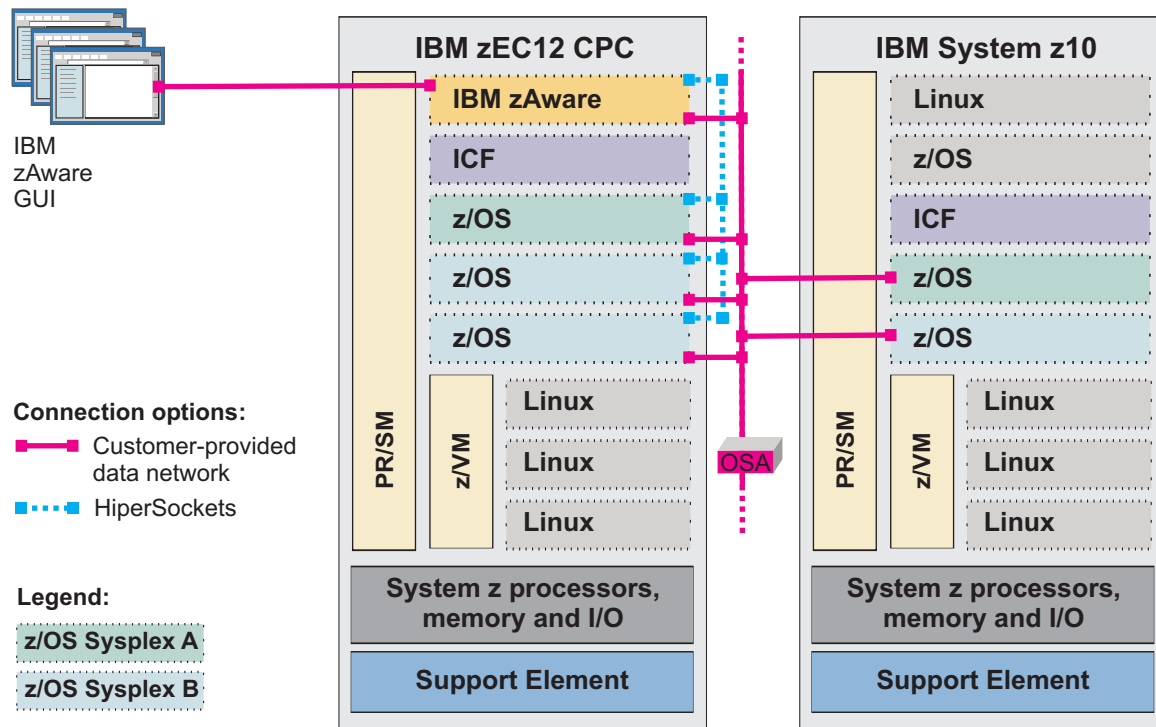


Figure 12. Network connections for an IBM zAware partition supporting clients in two zEC12 CPCs

When you configure the network connections for an IBM zAware partition, you select an IP address type for each connection: Dynamic Host Connection Protocol (DHCP), link local addressing, or static IPv4 or IPv6 address.

- With local link addressing and static IPv4 or IPv6 addresses, z/OS monitored clients and GUI users access the IBM zAware server through the dedicated IP address of the partition.
- With DHCP, the IP address of the partition can change. When you select a DHCP address type, you also must set up a domain name system (DNS) server to resolve a host name for the IBM zAware partition. With DHCP, both z/OS clients and GUI users need to use a host name rather than an IP address to successfully connect to the IBM zAware server.

To define the network connections, you need to modify configuration files for the zEC12 CPC, the IBM zAware partition, and z/OS monitored clients. Figure 13 on page 32 shows the configuration files that you need to modify.

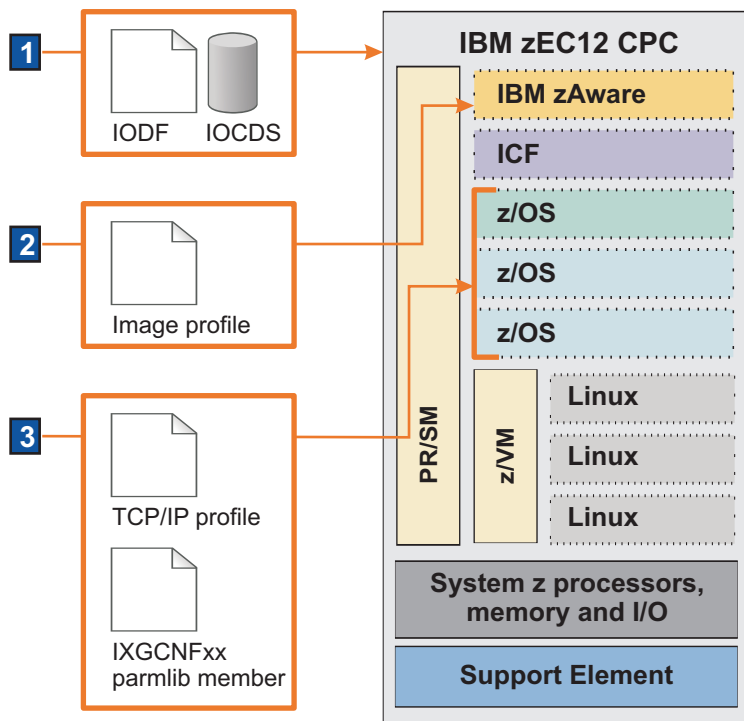


Figure 13. Configuration files for network connections

1. The I/O definition file (IODF) and input/output configuration data set (IOCDs) for the IBM zAware host system (zEC12 CPC) contain definitions that associate specific channel paths to the IBM zAware partition.

For optimal performance and operations, configure the IBM zAware partition such that it has access to only those channel path identifiers (CHPIDs), control units, and I/O devices that are required for network connectivity and storage. You can use the following HCD mechanisms to limit access:

- Image access and candidate lists in channel path definitions
- The explicit device candidate list for I/O devices

The supported channel path identifiers (CHPIDs) are:

- **OSD** for an OSA data network.
- **OSX** for the IEDN.
- **IQD** for HiperSockets or HiperSockets over the IEDN.

Channel paths can be dedicated, reconfigurable, shared, or spanned.

If you plan to configure monitored clients to use an existing HiperSockets subnet, for example, the IODF or IOCDs must include a CHPID type of **IQD** for the IBM zAware partition. The IODF or IOCDs also must include a channel path definition with an **OSD** type for GUI browser access to the IBM zAware server.

2. The image profile for the IBM zAware partition contains the IP address and host name of the partition, as well as network adapter definitions (such as the IP address type) for each type of network connection. These definitions correspond to the channel path types in the IODF or IOCDs. For example, to match the HiperSockets CHPID in the IODF or IOCDs, the image profile must include a network adapter definition with a CHPID type of **IQD**. That network adapter definition includes the IP address and other details about the HiperSockets subnet. Similarly, another network adapter definition with a CHPID type of **OSD** is required for GUI browser access to the IBM zAware server.
3. The TCP/IP profiles and system logger configuration settings for z/OS monitored clients also must contain specific network configuration settings.

- The TCP/IP profile must contain a statement that corresponds to the channel path types in the IODF or IOCDS for the IBM zAware host system.

For example, for connectivity through the HiperSockets subnet, the profile must contain a DEVICE and LINK MPCIPA statement with a device name of IUTIQDxx, where xx is the CHPID number that matches the hexadecimal value specified on the CHPID type IQD definition statement for the IBM zAware host system. Similarly, for GUI browser access to the IBM zAware server, the TCP/IP profile must contain an INTERFACE statement to define an IPAQENET or IPAQENET6 interface with CHPIDTYPE OSD.

Note: z/OS clients that use HiperSockets must be configured to use layer 3 (which is the default layer) or the client cannot successfully connect to the IBM zAware server. For these HiperSockets, the use of address resolution protocol (ARP) must be disabled. These restrictions do not apply for HiperSockets over the IEDN.

- The system logger configuration settings in the IXGCNFxx parmlib member must contain the following information:
 - The IP address or host name specified in the image profile for the IBM zAware partition.
 - The port number associated with the IBM zAware partition. The port number is 2001.

In summary, for each type of network connection that you want to use, you must have corresponding definitions in the configuration files. These corresponding definitions connect the IBM zAware partition and its monitored clients to the same network. The IBM zAware partition can be connected to more than one network, as necessary, to monitor z/OS systems at your installation.

- For additional information about the channel path types that the IBM zAware server supports, see “Summary of channel path types.”
- For a network planning checklist, see “Task summary and configuration checklist for network administrators” on page 34.

Summary of channel path types

Table 7 contains a summary of supported channel path types, usage, and sources of additional information.

Table 7. Supported channel path types for the IBM zAware partition

| Channel path type | Description | IBM zAware usage | Additional information |
|-------------------|---|---|---|
| OSD | Ethernet connectivity through an Open Systems Adapter (OSA) channel | <ul style="list-style-type: none"> • Use for monitored clients that reside on any supported System z CPC in the IBM zAware environment. • Use for GUI browser connections to the IBM zAware server. | zEnterprise System, System z10, System z9® and eServer™ zSeries Open Systems Adapter-Express Customer's Guide and Reference, SA22-7935 Note: For OSA-Express3 or later generation features, IBM zAware can use only port 0. |
| OSX | Connectivity through the intraensemble data network (IEDN) | Use only for monitored clients that reside on the IBM zAware host system or on other nodes in the same zEnterprise ensemble. | |
| IQD | Connectivity through HiperSockets | Use only for monitored clients that reside on the IBM zAware host system. Use the IQD channel path type for HiperSockets over the IEDN. | z/OS Communications Server: IP Configuration Guide, SC31-8775 |

Task summary and configuration checklist for network administrators

- Table 8 provides a summary of network administration tasks and links to additional information.
- Table 9 and Table 10 on page 35 are checklists that a network administrator can use to complete step 7 on page 75 in Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67.

Table 8. Task summary for network administrators

| ✓ | Task summary: | Where to find instructions: |
|---|---|---|
| | Collaborate with the security administrator to determine whether any additional network definitions are required to ensure secure communications between the IBM zAware server and its monitored clients. | “Securing communication between IBM zAware and its monitored clients” on page 51 |
| | Collaborate with the security administrator to determine whether any additional network definitions are required to ensure communication between the IBM zAware server and the Lightweight Directory Access Protocol (LDAP) server. | Your installation has the option to configure user authentication through the use of an LDAP repository. If there is a firewall between the IBM zAware partition and the LDAP server, the IBM zAware partition must be permitted to use the port that is used by the LDAP server. Also, if your installation uses a domain name instead of an explicit IP address for the LDAP server, the IBM zAware partition must be able to reach a DNS server for hostname-to-IP resolution. |
| | Define channel paths for networks in the I/O definition file (IODF) and input/output configuration data set (IOCDs) for the IBM zAware host system. | Step 1 on page 64 in Chapter 9, “Configuring network connections and storage for the IBM zAware partition,” on page 63 |
| | Define network settings in the image profile for the IBM zAware partition. | Step 7 on page 75 in Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67. |
| | Define network settings in the TCP/IP profile and system logger configuration file for each z/OS monitored client. | Steps 1 on page 92 and 3 on page 93 in Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91. |

Table 9. Checklist for IBM zAware partition network settings

| Network settings for the IBM zAware partition | | | | | | |
|---|--------------------------------------|------|-----------|-----------------|-------------------------|----------------------|
| ✓ | Host name or IP address ¹ | Port | Master ID | Default gateway | DNS server ² | Secondary DNS server |
| <i>Sample</i> | IBMzAWLPAR | 2001 | ZAIADMIN | 9.60.15.255 | 9.60.15.64 | — |
| | | | | | | |
| | | | | | | |

Footnotes:

1. Specify a host name if you select DHCP as the IP address type for the network adapter (channel path).
2. Specify a primary (and secondary, if appropriate) DNS server if you select DHCP as the IP address type for the network adapter (channel path).

Table 10. Checklist for IBM zAware partition network adapters

| Network adapters (channel paths) for the IBM zAware partition | | | | | | | |
|---|-------------------------|-------|--------------------------|------------------------------|------|------------|---------------|
| ✓ | CHPID type ¹ | CHPID | Interface or device name | IP address type ² | VLAN | IP address | Mask / prefix |
| Sample | OSD | 46 | OSAQDIO26 | DHCP | 1211 | 9.60.15.11 | 32 |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Footnotes:

1. One of the following: OSD (Ethernet connectivity over an OSA channel), OSX (intraensemble data network), or IQD (HiperSockets). The type determines which of the remaining columns you need to complete.
2. One of the following: DHCP, link local, static IPv4 or static IPv6 address. The type determines which of the remaining columns you need to complete.

Planning persistent storage configuration and capacity

To provide analytical data for monitored clients, IBM zAware requires continuous access to a set of Extended Count Key Data (ECKD™) direct-access storage devices (DASD). The number of storage devices in that set depends, in part, on the number of monitored clients in the IBM zAware environment and on the adjustable retention times that IBM zAware uses to manage stored data. Because of the way IBM zAware uses and depends on the availability of storage for its operation, careful planning is a critical phase for preparing to configure the IBM zAware environment.

IBM zAware stores the following analytical data on DASD:

- Current data from each monitored client, as well as priming data, if any.
- IBM zAware models for each monitored client.
- Analysis results for each monitored client.

IBM zAware sets default retention times for each of these types of analytical data and, through an automated process that runs daily, removes the data when the retention time has elapsed.

To plan for configuring and managing persistent storage use in an IBM zAware environment, review the following topics:

- “IBM zAware storage use and planning considerations” on page 36 describes IBM zAware storage use and dependencies that necessitate careful planning to avoid or quickly recover from potential storage-related problems.
- “Estimating required storage capacity and selecting devices” on page 38 provides guidelines for estimating and providing the persistent storage resources for your installation.
- Two examples provide an overview of the storage configuration process, along with the planning considerations for two different IBM zAware environments:
 - “Example: Storage configuration for normal operations” on page 39 describes how your installation might configure in-use and backup storage for a single instance of IBM zAware.
 - “Example: Storage configuration for multiple IBM zAware partitions” on page 42 describes how your installation might configure persistent storage for an IBM zAware environment that consists of:
 - One instance of IBM zAware (the primary) for normal operations.
 - Another instance of IBM zAware (the alternate) to be used in switchover situations.

An instance of IBM zAware is called an IBM zAware *server*.

- “Summary of planning considerations for persistent storage” on page 47 provides a summary of planning considerations, along with storage usage notes and best practices.
- “Task summary and configuration checklist for storage administrators” on page 49 provides a planning checklist for storage administrators.

IBM zAware storage use and planning considerations

To avoid or quickly recover from potential storage-related problems, storage administrators need to consider the information in Table 12 on page 48.

Table 11. Planning considerations and best practices for IBM zAware storage

| IBM zAware storage use | Why this fact is important for planning | Best practices |
|--|---|--|
| Through the I/O definition file (IODF) and input/output configuration data set (IOCDS) for the IBM zAware host system (zEC12 or zBC12 CPC), the IBM zAware partition has access to all storage devices that are physically attached to the CPC and defined to the same network connection that is defined for the partition. | <p>When the IBM zAware partition is activated, IBM zAware uses the IOCDS, and any existing IBM zAware storage configuration information, to populate the Data Storage page with a list of storage devices and their status (available, in use, and so on). Only when an administrator uses that list to select available devices to add to the storage configuration, IBM zAware formats and initializes the selected devices, overwriting any of the data that might be stored on those devices.</p> <p>Unless IBM zAware access is restricted to only specific CPC storage devices, an administrator might inadvertently cause the loss of critical data by adding a storage device that is not intended for IBM zAware use.</p> | <ul style="list-style-type: none"> • When defining storage devices in the IODF or IOCDS for the IBM zAware host system, the storage administrator can use image access and candidate lists for channel path definitions to allow only the IBM zAware partition to access specific devices. Using the explicit device candidate list is an alternative method of restricting access to specific devices. • As an additional precaution, you can use channel path definition lists, the explicit device candidate list, or operating system mechanisms to prevent the applications running in other CPC partitions from using storage devices that are intended for IBM zAware use. <p>The only exception to this practice is the CPC partition, if any, that your installation is using to back up the storage that the IBM zAware server is using.</p> |
| After IBM zAware formats and initializes storage devices for its use, the added devices constitute the in-use set of storage devices. Although IBM zAware tracks the status and capacity of individual storage devices that it is using, it treats the set of in-use devices as a single logical volume. | <p>If one or more individual devices become unavailable through any method other than removal through the IBM zAware GUI, IBM zAware effectively loses access to all of its stored data and operations stop.</p> <p>Only the following corrective actions can resolve this condition:</p> <ol style="list-style-type: none"> 1. If possible, try to reattach the device and reactivate the IBM zAware partition. 2. If the device cannot be reattached, you must replace it with an equivalent device containing a backup copy of the data that was stored on the unavailable device. The original device and the backup device must be the same size. 3. If your installation does not have backup copies of IBM zAware data, you must deactivate the IBM zAware partition and reconfigure the IBM zAware environment. | <ul style="list-style-type: none"> • If you must remove in-use devices from the CPC storage configuration, first use the IBM zAware GUI to remove those devices from the IBM zAware configuration. Then you can use other removal methods (such as changing the IOCDS) without affecting IBM zAware operations. • Because IBM zAware does not automatically replicate any of its stored data, creating and periodically updating a backup copy of this data is highly recommended. For replication, your installation can consider using IBM FlashCopy® or one of several Data Facility Storage Management Subsystem (DFSMS) copy services. • When replicating IBM zAware data from in-use data sets to backup data sets, remember to manage the backup set as a single entity. • When you use the IBM zAware GUI to replace a missing in-use device with its equivalent backup device, use the Preserve data option when adding the backup device, which prevents IBM zAware from overwriting data on the backup device. |

Figure 14 shows a configuration in which DASD attached to the IBM zAware host system has been configured exclusively for use by IBM zAware. Another partition in this configuration also can access the DASD, but only for the purpose of creating and periodically updating a backup copy of IBM zAware data.

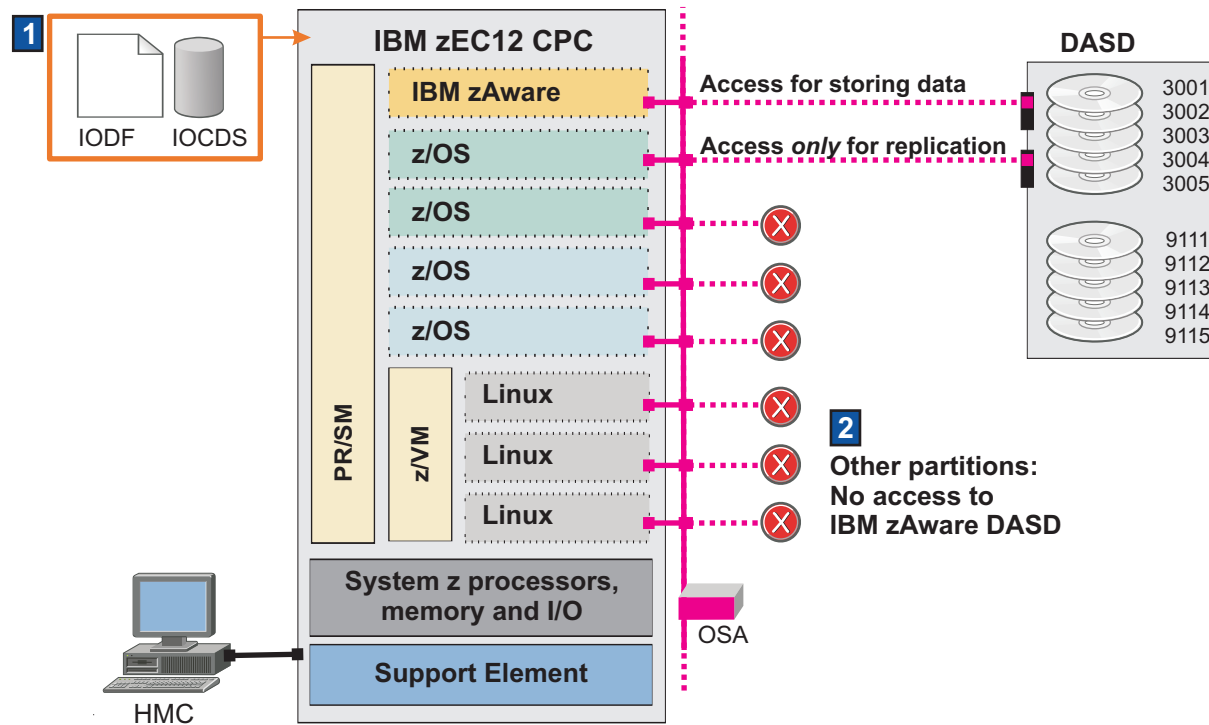


Figure 14. DASD configuration for normal operations, with access for one z/OS partition only to back up IBM zAware data

1. The I/O definition file (IODF) and input/output configuration data set (IOCDs) for the IBM zAware host system (zEC12 or zBC12 CPC) contain definitions for the physical storage devices that are attached to the CPC. Figure 14 shows only a subset of the DASD attached to the CPC.
 - Through the use of channel path definition lists, the storage administrator has configured this subset of DASD exclusively for use by the IBM zAware partition.
 - The storage administrator also has configured one additional partition to access the DASD, but only for the purpose of backing up IBM zAware data, which is a highly recommended practice. The system used for backing up data can reside on the IBM zAware host system or on another System z server in your installation.

For replication, your installation can consider using IBM FlashCopy or one of several Data Facility Storage Management Subsystem (DFSMS) copy services, including Extended Remote Copy (XRC) and Peer-to-Peer Remote Copy (PPRC) solutions. Another possible alternative is using DFSMSHsm to copy data, which requires deactivating the IBM zAware partition before copying data, then reactivating the partition after the copy operation completes. Non-IBM replication products also are available for use.
 2. Other partitions on the IBM zAware host system do not have access to the DASD that IBM zAware uses. Partitions that reside on other System z server in your installation also must not have access to storage devices that are exclusively for IBM zAware use.
- You can use channel path definition lists, the explicit device candidate list, or operating system mechanisms to prevent the applications running in other CPC partitions from using storage devices that are intended for IBM zAware use.

Estimating required storage capacity and selecting devices

Storage requirements vary depending on the retention times for each type of analytical data and on the number of monitored systems that you plan to connect to IBM zAware. Start with 500 GB of storage for IBM zAware to use, plus 4-5 GB of storage for each monitored system.

If you increase the number of monitored clients, you need to configure an additional 4-5 GB of storage for each monitored system. If you increase the retention times of instrumentation data, training models, or analysis results, you also might need to increase the amount of persistent storage that IBM zAware can use. To determine whether you need to add storage devices, periodically use the **Administration > Configuration > Data Storage** page to monitor the list of assigned storage devices, their current status, and capacity.

After estimating the required capacity, the storage administrator selects specific physical storage devices to reserve for the IBM zAware partition.

- Your installation can use Extended Count Key Data (ECKD) direct-access storage devices (DASD) to store IBM zAware data.
- Your installation can select a combination of small volumes or volumes of different sizes to provide the storage capacity that your IBM zAware environment requires. These volumes cannot be SMS-managed volumes.

- | • If any devices are to be used for storing backup copies of IBM zAware data, your installation must define two physically separate but equivalent sets of storage devices:
 - | – One set for IBM zAware to use for normal operations.
 - | – Another set for storing backup copies of data.

- | The number of storage devices in each set must match, and each backup device must be equivalent in size to the device from which the data is copied. These number and size requirements also apply for configurations that contain primary and alternate IBM zAware partitions.

- | After selecting specific physical storage devices, the storage administrator establishes and communicates conventions for persistent storage use to IBM zAware administrators. For example, suppose that your installation plans to set up an environment with one IBM zAware server, and plans to set up replication to copy its data. To implement this plan, the storage administrator might designate two sets of 3390 DASD for IBM zAware and communicate the following instructions and conventions:

- | • Use only devices 3001-3005 for normal operations.
- | • Devices 9111-9115 are reserved for replication. Naming conventions identify which backup device matches each in-use device; for example, 9111 contains the backup copy for data stored on 3001, 9112 contains the copy of data on 3002, and so on.
- | • If you change the set of in-use devices by adding or removing devices through the GUI, make sure that you adjust replication accordingly. To successfully replace an in-use device with its equivalent backup device, the set of in-use devices must match the set of backup devices in number of devices, size of devices, and content.

- | “Example: Storage configuration for normal operations” on page 39 illustrates how IBM zAware administrators can use these instructions and follow conventions to configure and manage IBM zAware storage.

Example: Storage configuration for normal operations

Figure 15 shows a sample IBM zAware environment that contains one IBM zAware partition. Although this figure shows a zEC12 as the host system, your installation can choose to host an IBM zAware partition on a zBC12 CPC.

Through the I/O definition file (IODF) and input/output configuration data set (IOCDs) for the IBM zAware host system, the partition has access to two physically separate sets of equivalent storage devices: 3001-3005 and 9111-9115. The storage administrator has designated devices 3001-3005 for IBM zAware data, and devices 9111-9115 to contain backup copies of that data. This type of configuration enables you to quickly restore IBM zAware operations after the loss of an in-use storage device, which can result from conditions such as a control unit failure on the device.

After the IBM zAware partition is activated, all of these devices are displayed as available for use through the Data Storage page in the IBM zAware graphical user interface (GUI). The numbered areas of Figure 15 illustrate the sequence of tasks that an IBM zAware administrator might follow to correctly configure these devices for normal operations and replication.

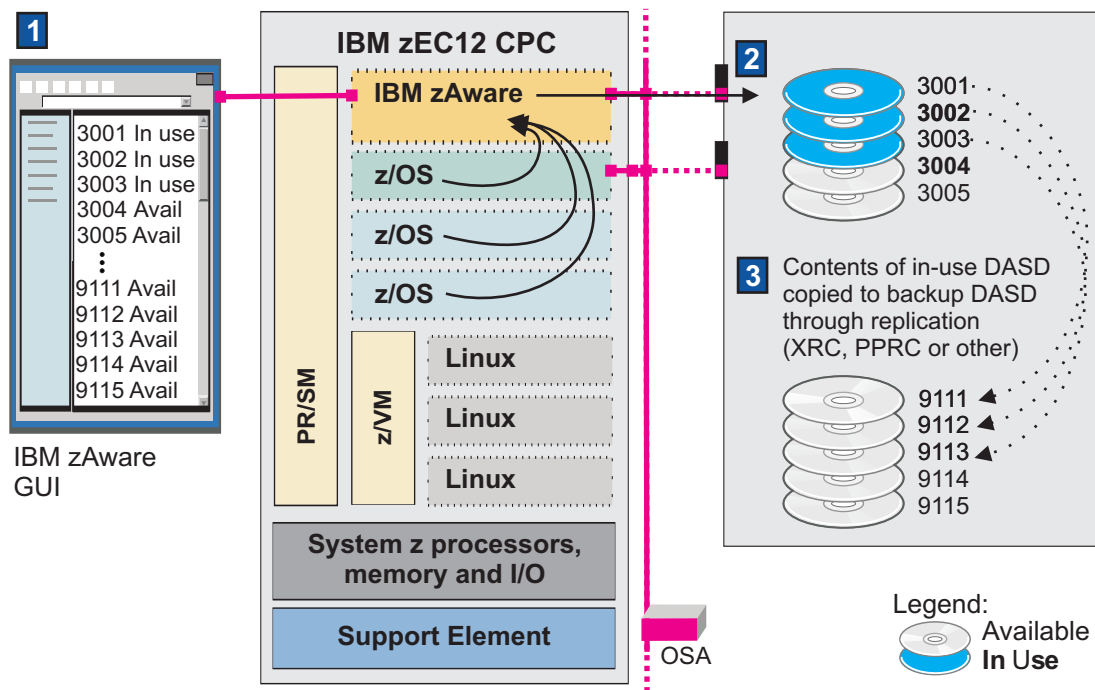


Figure 15. Storage configuration for the IBM zAware server for normal operations and data replication

- Using the Data Storage page in the IBM zAware GUI, an IBM zAware administrator selects devices for IBM zAware to use for normal operations. Before IBM zAware can store data in any of the 300x devices, an administrator must use the **Add and Remove Devices** function to select and add those storage devices.
 - For this sample configuration, an administrator has initially added only storage devices 3001-3003, reserving the other 300x devices for any additional capacity that might be needed when more monitored clients are added to the environment. This action causes IBM zAware to format and initialize the added devices. The GUI window depicted in Figure 15 shows the results of this selection process: the displayed status for devices 3001-3003 is now "In use".
 - Note that the administrator has *not* used **Add and Remove Devices** to configure the 911x devices, which are displayed in the GUI as "Available" devices. In a configuration that includes only one IBM zAware server, you cannot add backup devices until they are needed to replace an in-use device that is no longer available.

- | 2. With in-use devices available to store data, an administrator can finish configuring the IBM zAware environment by configuring and connecting monitored clients, sending priming data, and requesting IBM zAware to build models of client behavior.

| In Figure 15 on page 39, monitored clients that send data to IBM zAware are shown in partitions running on the IBM zAware host system, but additional monitored clients can run in partitions on other System z servers. IBM zAware parses and stores the following data on in-use devices 3001-3003:

- | • Current data from each monitored client, as well as priming data, if any.
- | • IBM zAware models for each monitored client.
- | • Analysis results for each monitored client.

- | 3. After normal IBM zAware operations begin, an administrator can set up replication for the in-use devices. For this replication to be successfully completed, both the number and sizes of devices in the backup set must match the number and sizes of in-use storage devices.

| For replication, your installation can consider using IBM FlashCopy or one of several Data Facility Storage Management Subsystem (DFSMS) copy services, including Extended Remote Copy (XRC) and Peer-to-Peer Remote Copy (PPRC) solutions. Another possible alternative is using DFSMSHsm to copy data, which requires deactivating the IBM zAware partition before copying data, then reactivating the partition after the copy operation completes. Non-IBM replication products also are available for use.

| Figure 15 on page 39 shows that one of the monitored clients, the z/OS partition highlighted in light green, has access to IBM zAware in-use storage devices 3001-3005, as well as their equivalent backup set of devices, 9111-9115. An administrator has set up this z/OS image to periodically run a job that copies data from the set of in-use devices to the backup set:

- | • Device 9111 contains a copy of the data from device 3001.
- | • Device 9112 contains a copy of the data from device 3002.
- | • Device 9113 contains a copy of the data from device 3003.

| If you change the set of in-use devices by adding or removing devices through the GUI, make sure that you adjust replication accordingly. To successfully replace an in-use device with its equivalent backup device, the set of in-use devices must match the set of backup devices in number of devices, size of devices, and content.

| Figure 16 on page 41 illustrates how this backup data can be used when an in-use storage device becomes unavailable. Starting from the right side of the figure, the numbered areas illustrate the sequence of events and recovery tasks that an IBM zAware administrator can follow to resolve a “missing in-use device” condition.

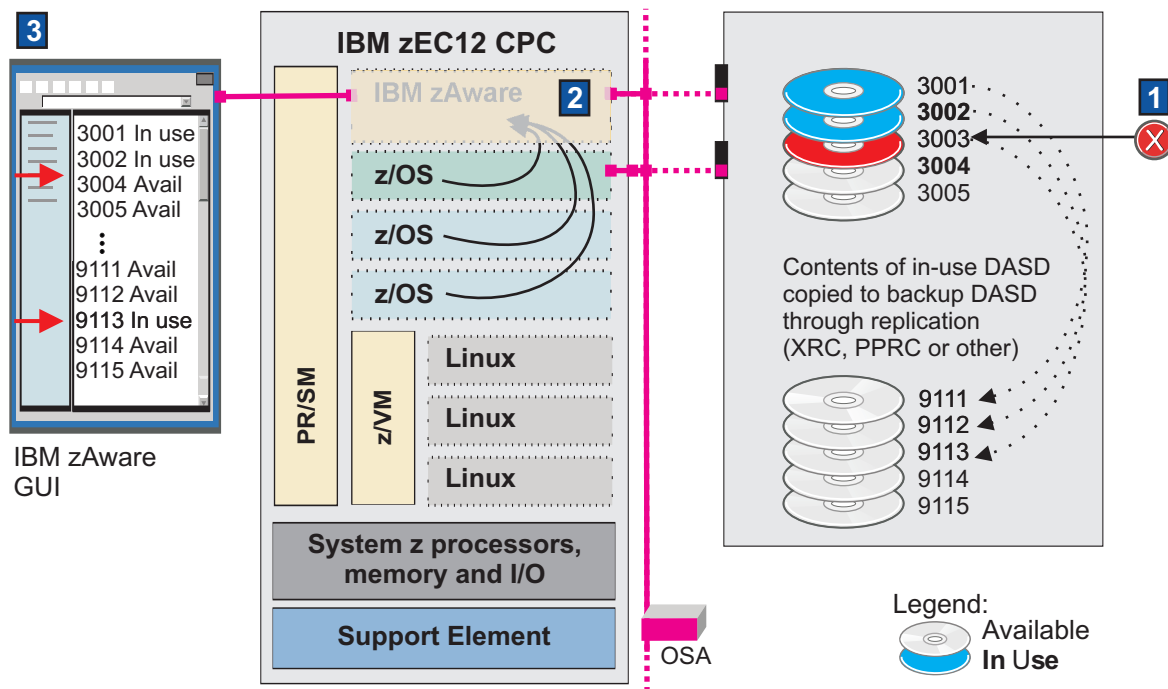


Figure 16. What happens when an in-use storage device becomes unavailable

1. In-use storage device 3003 is no longer attached to the IBM zAware partition. It might have been removed or disconnected through storage operations that are not provided through the Data Storage page of the IBM zAware GUI, such as:
 - Replacing the I/O definition file (IODF) for the host system with an IODF that does not contain the in-use storage devices for IBM zAware.
 - Using the Support Element (SE) to take offline one or more channel paths (CHPIDs) for storage devices or for the network through which those devices are connected to the IBM zAware partition.
2. When an in-use storage device becomes unavailable, IBM zAware operations stop. To a user of the IBM zAware GUI, the GUI appears to hang. On the SE for the IBM zAware host system, hardware messages indicate input/output (I/O) problems related to the loss of access to physical storage devices.

At this point, an IBM zAware administrator can take only the following corrective actions to resolve this condition:

 - a. If possible, try to reattach the device and reactivate the IBM zAware partition.
 - b. If the device cannot be reattached, you must replace it with an equivalent device containing a backup copy of the data that was stored on the unavailable device. The original device and the backup device must be the same size.
 - c. If your installation does not have backup copies of IBM zAware data, you must deactivate the IBM zAware partition and reconfigure the IBM zAware environment.
3. Assuming that the administrator could not reattach missing device 3003 but was able to reactivate the IBM zAware partition, the administrator can replace device 3003 with its equivalent: device 9113.
 - a. When the administrator first logs in to the GUI, IBM zAware presents the Data Storage page with message AIFP0013E, which indicates the missing device condition.
 - b. From the Data Storage page, the administrator clicks **Add and Remove Devices** to select the replacement device. The Add and Remove Devices window contains the **Preserve data** option, which is shown in Figure 17 on page 42. This option is intended for use *only* when adding a storage device that contains replicated data from an in-use device.

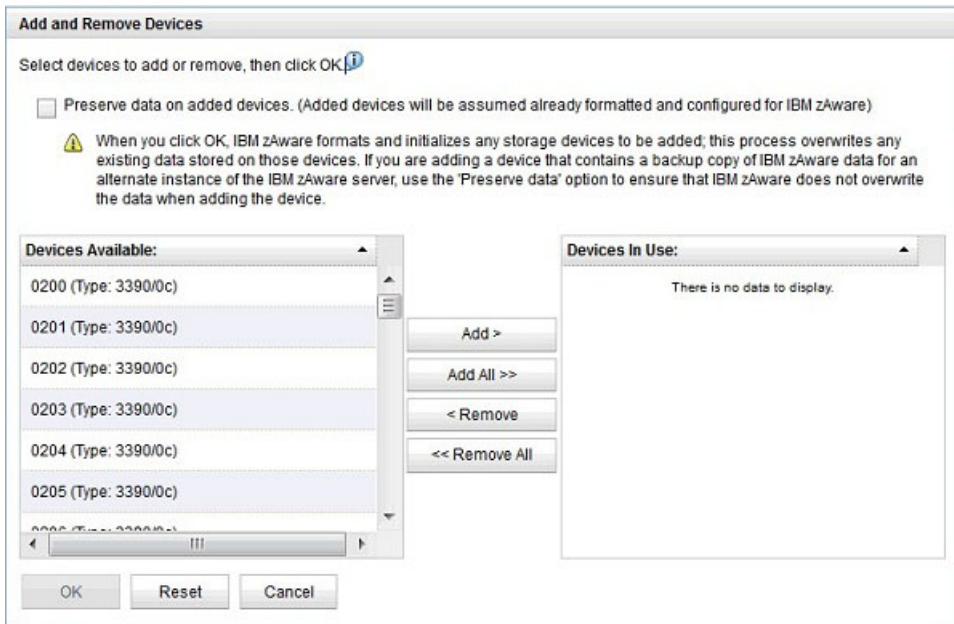


Figure 17. The **Preserve data** option on the Add and Remove Devices window

- c. The administrator selects both the **Preserve data** option and device 9113, then clicks **Add** to add 9113 to the list of in-use storage devices. Because the **Preserve data** option was selected, IBM zAware does *not* format 9113 so the replicated data on that device is preserved and usable.

The GUI window depicted in Figure 16 on page 41 shows the results of the missing device condition and the administrator's corrective action:

- Device 3003 is no longer listed in the Data Storage Devices table.
- Device 9113 is listed as an in-use device.

If the replicated data on a backup device is back-level, IBM zAware cannot provide analytical data for the dates between the last day of replication and the date when the in-use storage device became unavailable. Also, during the time between the detection of the missing device condition and its successful resolution, any data that monitored clients attempt to send to IBM zAware is lost. If you consider this missing data to be critical for analyzing monitored clients, you can use the z/OS bulk load client for IBM zAware to resend any client OPERLOG data that might be missing.

Example: Storage configuration for multiple IBM zAware partitions

Your installation can configure more than one IBM zAware partition, with one for normal operations and another reserved for switchover situations. This type of configuration enables you to quickly restore IBM zAware operations after a failure.

- To quickly recover from a control unit (CU) failure on a storage device, set up an alternate IBM zAware on either the same or a different host system.
- To quickly recover from a central processor complex (CPC) failure, set up an alternate IBM zAware on a different host system. The alternate host system might have the IBM zAware disaster recovery (DR) feature installed, but this feature is not required.

When your installation configures a primary IBM zAware partition and an alternate IBM zAware partition for switchover situations, only one IBM zAware server can be active at a given time but both servers must have access to the same data.

- To correctly configure the partition in which the alternate server runs, use the same IP address as you defined for the primary partition. Doing so guarantees that you cannot have multiple IBM zAware

servers running simultaneously, and also eliminates the need to reconfigure the TCP/IP settings of monitored clients if you have to switch from using the primary server to the alternate server.

- To correctly configure persistent storage for primary and alternate IBM zAware partitions, your installation must define physically separate but equivalent sets of storage devices for each partition, and also set up replication to copy the content of the primary storage devices to the alternate storage devices. For data replication to be successful, the number of storage devices in the primary set must match the number of devices in the alternate set. Additionally, each alternate device must be equivalent in size to the primary device.

The series of figures in this topic illustrate how to configure storage for a primary IBM zAware server and an alternate server that reside in separate host systems. For this example, assume that the storage administrator has designated devices 3001-3005 for IBM zAware data, and devices 9111-9115 to contain backup copies of that data.

Figure 18 shows the configuration for the primary IBM zAware server. Through the I/O definition file (IODF) and input/output configuration data set (IOCDS) for the IBM zAware host system (zEC12 or zBC12 CPC), the partition has access to *only one* of the two physically separate sets of equivalent storage devices: 3001-3005. After the IBM zAware partition is activated, only the 300x devices are displayed as available for use through the Data Storage page in the IBM zAware graphical user interface (GUI). The numbered areas of Figure 18 illustrate the sequence of tasks that an IBM zAware administrator might follow to correctly configure these devices for normal operations and replication.

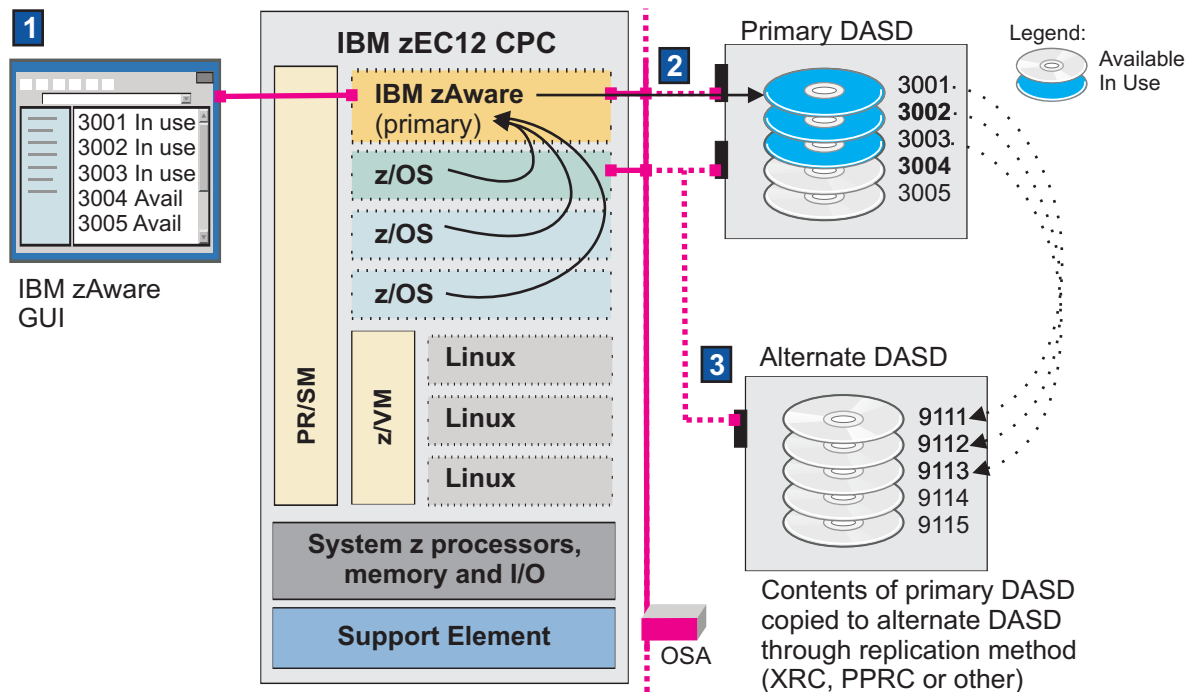


Figure 18. DASD configuration for the primary IBM zAware server on one host system

1. Using the Data Storage page in the IBM zAware GUI, an IBM zAware administrator selects devices for the primary IBM zAware server to use for normal operations. Note that only the 300x devices are listed in the GUI as available for use by the primary server.
Before IBM zAware can store data in any of the 300x devices, an administrator must use the **Add and Remove Devices** function to select and add those storage devices. This action causes IBM zAware to format and initialize the added devices.
For this sample configuration, an administrator has initially added only storage devices 3001-3003, reserving the other 300x devices for any additional capacity that might be needed when more

monitored clients are added to the environment. The GUI window depicted in Figure 18 on page 43 shows the results of this selection process: the displayed status for devices 3001-3003 is now “In use”.

2. With in-use devices available to store data, an administrator can finish configuring the primary IBM zAware environment by configuring and connecting monitored clients, sending priming data, and requesting IBM zAware to build models of client behavior.

In Figure 18 on page 43, monitored clients that send data to the primary IBM zAware server are shown in partitions running on the same host system, but additional monitored clients can run in partitions on other System z servers. IBM zAware parses and stores the following data on in-use devices 3001-3003:

- Current data from each monitored client, as well as priming data, if any.
- IBM zAware models for each monitored client.
- Analysis results for each monitored client.

3. After normal IBM zAware operations begin, an administrator can set up replication for the in-use devices. For this replication to be successfully completed, both the number and sizes of devices in the backup set match the number and sizes of in-use storage devices.

For replication, your installation can consider using IBM FlashCopy or one of several Data Facility Storage Management Subsystem (DFSMS) copy services, including Extended Remote Copy (XRC) and Peer-to-Peer Remote Copy (PPRC) solutions. Another possible alternative is using DFSMSHsm to copy data, which requires deactivating the IBM zAware partition before copying data, then reactivating the partition after the copy operation completes. Non-IBM replication products also are available for use.

Figure 18 on page 43 shows that one of the monitored clients, the z/OS partition highlighted in light green, has access to IBM zAware in-use storage devices 3001-3005, as well as their equivalent backup set of devices, 9111-9115.

An administrator has set up this z/OS image to periodically run a job that copies data from the set of in-use devices to the backup set:

- Device 9111 contains a copy of the data from device 3001.
- Device 9112 contains a copy of the data from device 3002.
- Device 9113 contains a copy of the data from device 3003.

With backup devices and data available for the primary IBM zAware server, an administrator can set up the alternate server to prepare for potential switchover situations. The numbered areas of Figure 19 on page 45 illustrate the sequence of tasks that an administrator follows to correctly configure the alternate IBM zAware server.

- d. Except for the storage devices to be added, the configuration of the alternate server can exactly match that of the primary server. For example, if your installation is using an existing Lightweight Directory Access Protocol (LDAP) server for user authentication to the primary server, the administrator can configure the same LDAP server for use with the alternate server.

After the persistent storage and security configuration for the alternate server is complete, the administrator completes the following steps to reactivate the primary IBM zAware environment:

1. Deactivate the alternate IBM zAware partition.
2. Reactivate the primary IBM zAware partition.
3. Reconnect the monitored clients.

During the course of normal operations, an administrator might need to change the set of in-use devices for the primary server by adding or removing devices through the GUI. Because the in-use set and backup set of devices must be equivalent for a switchover to be successful, the administrator also must adjust replication and the set of storage devices for the alternate server so both of the primary and alternate sets match in number of devices, size of devices, and content.

After an administrator completes the initial configuration of both the primary and alternate servers, either IBM zAware server can detect and report mismatches only when its partition is activated. Remember that only one IBM zAware server can be active at a given time. The following example illustrates how, on activation, the primary IBM zAware reports mismatches between its set of in-use devices and the set of devices for the alternate IBM zAware server. Similarly, on activation, the alternate IBM zAware can detect and report mismatches between its set of in-use devices and the primary set.

- If a mismatch occurs because the administrator removed a device from the alternate set, the activated primary IBM zAware server issues message AIFP0012I to indicate that a device was removed from the alternate set, and takes corrective action by removing the equivalent device from its in-use set of devices. In this case, no administrator intervention is required.
- If a mismatch occurs because the administrator added a device to the alternate set, the activated primary IBM zAware issues message AIFP0013E to indicate that a device is missing from its in-use set. In this case, IBM zAware operations stop until an administrator successfully adds an equivalent device to the storage configuration of the primary IBM zAware server.

Figure 20 on page 47 illustrates how an administrator can switch the IBM zAware environment from the primary to the alternate server when a switchover situation occurs.

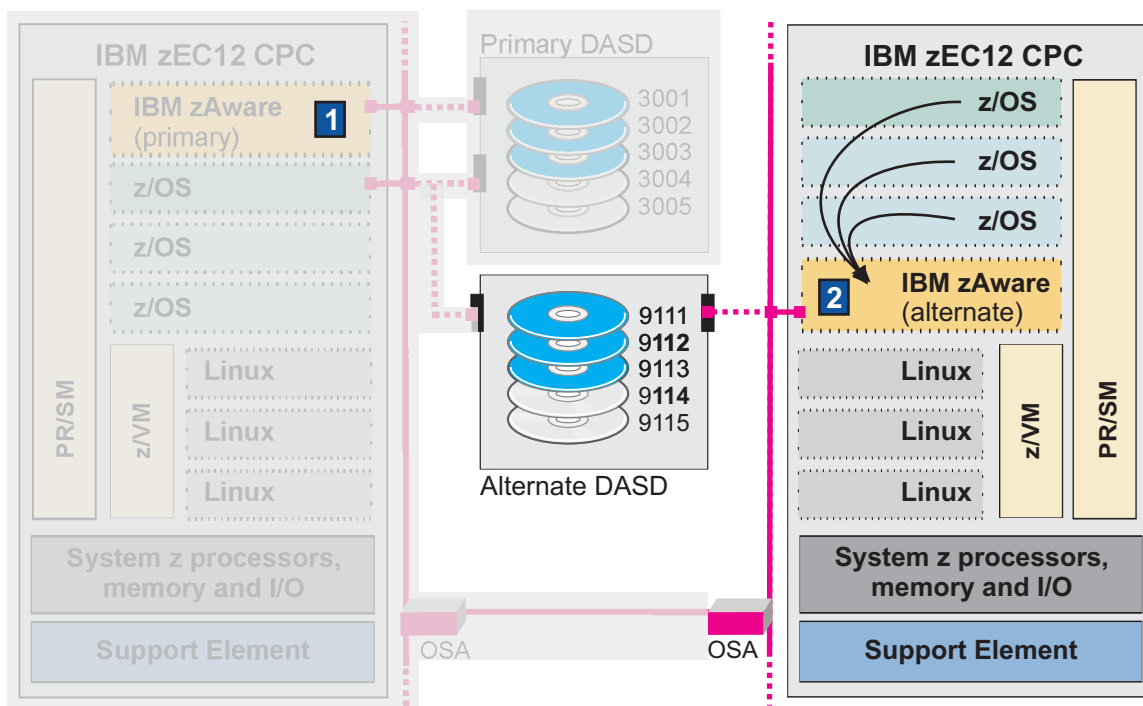


Figure 20. What happens when a switchover situation occurs

1. The host system for the primary IBM zAware experiences a CPC failure. IBM zAware operations stop. To a user of the IBM zAware GUI, the GUI appears to hang.
 2. The administrator activates the alternate IBM zAware on its host system. Because its configuration is the same as that of the primary, with the exception of storage devices, the administrator can reIPL the monitored clients and reconnect them to the alternate server.
- Depending on the timing of the CPC failure and the replication schedule for backing up IBM zAware data, the data on devices 9111-9113 might be back-level. In this case, the alternate IBM zAware cannot provide analytical data for the dates between the last day of replication and the date and time when the administrator switched the IBM zAware environment to the alternate CPC.

Summary of planning considerations for persistent storage

Table 12 on page 48 provides a summary of planning considerations and best practices for IBM zAware storage configuration.

Table 12. Planning considerations and best practices for IBM zAware storage configuration

| Planning consideration | Usage notes and best practices |
|--|--|
| Storage device requirements | <ul style="list-style-type: none"> Your installation can use Extended Count Key Data (ECKD) direct-access storage devices (DASD) to store IBM zAware data. Your installation can select a combination of small volumes or volumes of different sizes to provide the storage capacity that your IBM zAware environment requires. These volumes cannot be SMS-managed volumes. If any devices are to be used for storing backup copies of IBM zAware data, your installation must define two physically separate but equivalent sets of storage devices: <ul style="list-style-type: none"> One set for IBM zAware to use for normal operations. Another set for storing backup copies of data. <p>The number of storage devices in each set must match, and each backup device must be equivalent in size to the device from which the data is copied. These number and size requirements also apply for configurations that contain primary and alternate IBM zAware partitions.</p> |
| Partition access to storage devices | <ul style="list-style-type: none"> When defining storage devices in the IODF or IOCDS for the IBM zAware host system, the storage administrator can use image access and candidate lists for channel path definitions to allow only the IBM zAware partition to access specific devices. Using the explicit device candidate list is an alternative method of restricting access to specific devices. As an additional precaution, you can use channel path definition lists, the explicit device candidate list, or operating system mechanisms to prevent the applications running in other CPC partitions from using storage devices that are intended for IBM zAware use. <p>The only exception to this practice is the CPC partition, if any, that your installation is using to back up the storage that the IBM zAware server is using.</p> |
| Minimum storage amount and the number of monitored clients | <p>Storage requirements vary depending on the retention times for each type of analytical data and on the number of monitored systems that you plan to connect to IBM zAware. Start with 500 GB of storage for IBM zAware to use, plus 4-5 GB of storage for each monitored system.</p> <p>If you increase the number of monitored clients, you need to configure an additional 4-5 GB of storage for each monitored system.</p> |
| Adjustable retention times for stored data | <p>IBM zAware stores the following analytical data on DASD:</p> <ul style="list-style-type: none"> Current data from each monitored client, as well as priming data, if any. IBM zAware models for each monitored client. Analysis results for each monitored client. <p>IBM zAware sets default retention times for each of these types of analytical data and, through an automated process that runs daily, removes the data when the retention time has elapsed. Reducing these default retention times might reduce the amount of storage you need to configure for IBM zAware; if necessary, you can reduce the default retention times through the Administration > Configure Settings > Analytics page in the IBM zAware GUI.</p> |

Table 12. Planning considerations and best practices for IBM zAware storage configuration (continued)

| Planning consideration | Usage notes and best practices |
|----------------------------------|--|
| Backup copies of IBM zAware data | <p>Creating and periodically updating a backup copy of IBM zAware data is recommended for the following reasons:</p> <ul style="list-style-type: none"> • IBM zAware does not automatically replicate any of its data. • If a storage device is damaged, disconnected, or removed from the CPC, IBM zAware effectively loses access to its data and cannot continue to analyze data from monitored clients. Only the following corrective actions can resolve this condition: <ol style="list-style-type: none"> 1. If possible, try to reattach the device and reactivate the IBM zAware partition. 2. If the device cannot be reattached, you must replace it with an equivalent device containing a backup copy of the data that was stored on the unavailable device. The original device and the backup device must be the same size. 3. If your installation does not have backup copies of IBM zAware data, you must deactivate the IBM zAware partition and reconfigure the IBM zAware environment. <p>Guidelines for configuring and managing backup devices and data:</p> <ul style="list-style-type: none"> • If any devices are to be used for storing backup copies of IBM zAware data, your installation can define physically separate but equivalent sets of storage devices, one set for IBM zAware to use for normal operations (the in-use set), and another set for storing backup copies of data. The number of storage devices in the in-use set must match the number of devices in the backup set. Additionally, each backup device must be equivalent in size to the in-use device. • The same number and size requirements apply for configurations containing primary and alternate IBM zAware servers. Your installation must define physically separate but equivalent sets of storage devices for each server, with the same number of storage devices in the primary set and the alternate set. Additionally, each alternate device must be equivalent in size to the primary device. • For replication, your installation can consider using IBM FlashCopy or one of several Data Facility Storage Management Subsystem (DFSMS) copy services, including Extended Remote Copy (XRC) and Peer-to-Peer Remote Copy (PPRC) solutions. Another possible alternative is using DFSMSHsm to copy data, which requires deactivating the IBM zAware partition before copying data, then reactivating the partition after the copy operation completes. Non-IBM replication products also are available for use. • If you change the set of in-use devices by adding or removing devices through the GUI, make sure that you adjust replication accordingly. To successfully replace an in-use device with its equivalent backup device, the set of in-use devices must match the set of backup devices in number of devices, size of devices, and content. This requirement also applies when switching between primary and alternate IBM zAware servers. • If the replicated data on a backup device is back-level, IBM zAware cannot provide analytical data for the dates between the last day of replication and the date and time when the administrator replaced an in-use storage device with its equivalent backup device. |

Task summary and configuration checklist for storage administrators

- Table 13 on page 50 provides a summary of storage administration tasks and links to additional information.
- Table 14 on page 50 is a checklist that a storage administrator can use to complete step 2 on page 65 in Chapter 9, “Configuring network connections and storage for the IBM zAware partition,” on page 63.

Table 13. Task summary for storage administrators

| ✓ | Task summary: | Where to find instructions: |
|---|--|---|
| | Configure persistent storage for the IBM zAware partition through the Hardware Configuration Definition (HCD). | Step 2 on page 65 in Chapter 9, “Configuring network connections and storage for the IBM zAware partition,” on page 63 |
| | Assign storage devices for the IBM zAware server through the Administration > Configuration > Data Storage page in the IBM zAware graphical user interface (GUI). | Step 2 on page 81 in Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79 |
| — | Manage storage devices that the IBM zAware server is using through the GUI Administration > Configuration > Data Storage page. | “Adding and removing storage devices” on page 145 |
| — | (Optional but highly recommended) Periodically use the replication method of your choice to back up the storage devices that the IBM zAware server is using | The product documentation for the replication method that you choose. If you are using a DFSMS copy service or DFSMSshm, see the relevant z/OS DFSMS topics in the z/OS Information Center at this URL: http://publib.boulder.ibm.com/infocenter/zos/v1r13/ |
| | (Optional) Configure an alternate IBM zAware partition for use in switchover situations | Chapter 21, “Setting up multiple IBM zAware partitions for switchover situations,” on page 187 |

Table 14. Checklist for Extended Count Key Data (ECKD) storage devices

| Extended Count Key Data (ECKD) storage devices | | | | | | |
|---|------------|-------------------|--------|----------|---------------|---------------|
| ✓ | Name | Size ¹ | Type | Location | Device number | Volume serial |
| Sample | PoolEckd01 | 10017 | 3390-9 | SYSTEM1 | 9051 | AC3231 |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Backup storage devices² | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Footnotes: 1. The size in cylinders for ECKD devices. Only numbers 0-9 are allowed. The maximum value is $2^{63} - 1$ (9,223,372,036,854,775,807). 2. To store backup copies of IBM zAware data through replication, provide one backup device for each in-use device; the backup device must match the size of the in-use device. | | | | | | |

Chapter 6. Planning for security

IBM zAware does not require clients to provide authentication credentials or to encrypt the operations log (OPERLOG) data that they send. If your installation considers this data to be sensitive, you need to ensure that the communication between IBM zAware and its monitored clients occurs over secured networks that are configured with preexisting security mechanisms. IBM zAware does provide security mechanisms through which you can limit access to the IBM zAware graphical user interface (GUI), through which users can view the analytical data for clients and modify the operational controls for the IBM zAware server.

Securing communication between IBM zAware and its monitored clients

As stated and illustrated in Chapter 4, “Planning your IBM zAware environment,” on page 19, the recommended configuration for an IBM zAware environment is contained within a single security zone protected by a firewall.

For a z/OS monitored client to be correctly configured, the z/OS system logger must have Security Authorization Facility (SAF) authorization to send data to the IBM zAware server. Additional security options, which you can use for authentication, data privacy, and data integrity, depend on the type of network connection that the server and clients use. As noted in “Planning network connections and capacity” on page 29, the supported network connections are:

- Ethernet connectivity through an Open Systems Adapter (OSA) channel. If you are using an OSA channel for the IBM zAware environment, you can restrict access to the server and client IP addresses or to specific networks by using SERVATH and NETACCESS profiles.

Using NETACCESS statements, z/OS Communications Server can map networks, subnetworks and IP addresses to SAF resource names. Users that are not permitted access to a particular SAF resource are not allowed to communicate with the corresponding network, subnetwork, or IP address.

If you are using the OSX channel type for the IBM zAware environment, you can implement a virtual local area network (VLAN) to enforce isolation between networks.

- Connectivity through the intraensemble data network (IEDN). If you are using the IEDN for the IBM zAware environment, you can implement VLANs to enforce isolation between networks.
- Connectivity through HiperSockets. If you are using HiperSockets, you can implement VLANs to enforce isolation between networks. Because a HiperSocket is an in-memory socket, it inherits the normal System z memory protections.

- | **Firewall consideration:** If communication from remote monitored clients must pass through a firewall to the IBM zAware server, you might need to configure the firewall to allow incoming connections to the server on port 2001. For additional information about securing network connections, see *z/OS Communications Server IP Configuration Guide*, SC31-8775.

Securing communication between IBM zAware and GUI users

IBM zAware provides the following security mechanisms that your installation can configure to limit access to the IBM zAware GUI.

Master user ID and password

- | Your installation defines the master user ID on the **zAware** page of the image profile of the IBM zAware partition. The password does not expire and IBM zAware does not provide any mechanism that requires you to change the password on a regular basis. If you forget the password, you can restore access by setting a new default user ID and password through the **zAware** page of the image profile.

After configuring the IBM zAware environment and activating the IBM zAware partition, you must use the default master user ID to initially log in to the IBM zAware GUI. This master user ID has authority to perform any task that is available through the IBM zAware GUI.

Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67 provides instructions for using the Hardware Management Console (HMC) to define the master user ID in the image profile of the partition.

Server SSL certificate

A Secure Sockets Layer (SSL) certificate is automatically generated for IBM zAware when your installation performs the initial activation of the IBM zAware partition. This certificate is not signed by a certificate authority (CA); therefore, the first time you log in to the IBM zAware graphical user interface (GUI), the browser displays a warning message because it does not recognize the default SSL certificate. You can resolve this problem by replacing the default SSL certificate with a certificate signed by a certificate authority of your choice. Doing so provides secure communication between the IBM zAware server and the browsers of all authorized users.

If you do not replace the automatically generated certificate, users can bypass the browser error message by adding a security exception, but cannot verify that they are connected to a legitimate IBM zAware partition. The automatically generated certificate is valid for one year from the initial activation of the IBM zAware partition, and is automatically renewed according to WebSphere® Application Server certificate expiration settings, as described at the following URL.

http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=%2Fcom.ibm.websphere.base.doc%2Finfo%2Faes%2Fae%2Fsec_sslmancertexpir.html

If you decide to replace the automatically generated certificate, which is the recommended practice for improved security, you can use any third-party certificate authority of your choice, or your installation can provide an internal certificate authority for certificate signing tasks. IBM zAware does not renew these replacement certificates; in this case, managing replacement certificates becomes the responsibility of the security administrator. The Open Directory Project maintains a list of third-party certificate authorities at the following URL.

http://www.dmoz.org/Computers/Security/Public_Key_Infrastructure/PKIX/Tools_and_Services/Third_Party_Certificate_Authorities/

The required format for replacement certificates is Base64 encoded X509 certificate blocks.

Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79 provides instructions for replacing the default self-signed SSL certificate, and provides sample certificate blocks to illustrate the content that you might receive from a certificate authority. When you receive a reply from a certificate authority, the reply might contain a chain of certificates, starting with the signed server certificate, possibly followed by certificates from one or more intermediate CAs and, finally, the self-signed certificate of the CA. When you supply this information in the GUI, provide the entire certificate chain, starting with the signed server certificate through the self-signed certificate of the CA.

In some cases, the CA reply that you receive is delivered in a public-key cryptography standards (PKCS) #7 file. You must extract the certificates from the file before pasting them into the GUI. One method of extracting certificates from a PKCS #7 file is to use the **openssl pkcs7** command; for more information, see the OpenSSL Project web site at the following URL.

<http://www.openssl.org/>

User authentication for the IBM zAware GUI

You can authorize users to access the IBM zAware server through the use of an existing Lightweight Directory Access Protocol (LDAP) repository or, alternatively, through the use of a local file-based repository.

For simplicity, using an LDAP repository only is the preferred option. However, you might want to define one or two user IDs in a local repository so you can access the IBM zAware GUI when the LDAP server is unavailable. If you configure an LDAP repository and also define users or

groups in a local repository, both sets of users or groups are available through the IBM zAware GUI. Do **not** define the same user ID in more than one repository; results are unpredictable.

- The IBM zAware GUI provides pages through which you can configure an LDAP repository. Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79 provides instructions for configuring an LDAP repository through the IBM zAware GUI.
- To use a local file-based repository instead of an LDAP repository, use the instructions in Chapter 20, “Setting up a local repository to secure access to the IBM zAware GUI,” on page 185.

Use the WebSphere Application Server Integrated Solutions Console to add users or groups to, or remove them from, the repository.

Attention: Do not perform any operations other than user and group management through the Integrated Solutions Console. In particular, do not change any options under the Security section, including changes related to LDAP configuration. Configuration changes in these areas do not persist across activations of the IBM zAware partition and thus might cause the loss of IBM zAware functions.

For more information about repositories, see the topic on federated repositories in the WebSphere Application Server information center at this URL:

<http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?>

Role-based access to IBM zAware GUI functions

To grant access to the GUI, you need to map authorized users and groups to specific roles: either **Administrator** or **User**. User IDs or groups that are assigned to the Administrator role can access and use any task in the GUI, including those listed under **Administration** in the GUI navigation tree. Administrators have the authority to customize the IBM zAware environment and operations; for example:

- Through the **Analytics** page, an administrator can change data retention and training values that affect analytical operations.
- Through the **Data Storage** page, an administrator can add to or remove storage devices from the IBM zAware configuration.
- Through the **Security** page, an administrator can configure user authentication controls.

User IDs or groups that are assigned to the User role cannot view any of the pages under **Administration** in the GUI navigation tree. User IDs or groups assigned to the User role can view only the following pages and use only the actions as noted:

- On the graphic or tabular **Analysis** page, all controls and actions are permitted.
- On the **Interval view**, all controls and actions are permitted except for modifying the non-IBM rules status for a specific message ID. Only administrators can view and change a rules status value. IBM rules cannot be changed.
- On the **Notifications** page, all actions are disabled.
- On the **System Status** page, all actions are disabled.

Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79 provides instructions for mapping user IDs or groups to specific roles.

Browser session timeout setting

By default, browser sessions time out after 12 hours (720 minutes). Your installation can change this setting through the **LTPA Settings** tab on the **Administration > Configuration > Security** page in the IBM zAware GUI.

Task summary for security administrators

Table 15 provides a summary of security administration tasks and links to additional information.

Table 15. Task summary for security administrators

| ✓ | Task summary: | Where to find instructions: |
|---|--|---|
| | Collaborate with the network administrator if you have determined that additional network definitions are required to ensure secure communications between the IBM zAware server and its monitored clients. | <ul style="list-style-type: none"> Additional security options, which you can use for authentication, data privacy, and data integrity, depend on the type of network connection that the server and clients use. If communication from remote monitored clients must pass through a firewall to the IBM zAware server, you might need to configure the firewall to allow incoming connections to the server on port 2001. <p>For additional information about securing network connections, see <i>z/OS Communications Server IP Configuration Guide</i>, SC31-8775.</p> |
| | Collaborate with the network administrator to determine whether any additional network definitions are required to ensure communication between the IBM zAware server and the Lightweight Directory Access Protocol (LDAP) server. | Your installation has the option to configure user authentication through the use of an LDAP repository. If there is a firewall between the IBM zAware partition and the LDAP server, the IBM zAware partition must be permitted to use the port that is used by the LDAP server. |
| | (Optional) Secure the communication between the IBM zAware server and browsers by requesting and importing a digital certificate. | Step 3 on page 83 in Chapter 11, "Configuring storage, security, and analytics for the IBM zAware server," on page 79. |
| | Configure the LDAP repository or a local file-based repository for storing user access information. | Step 4 on page 84 in Chapter 11, "Configuring storage, security, and analytics for the IBM zAware server," on page 79. |
| | Authorize users or groups to access the IBM zAware GUI. | Step 5 on page 87 in Chapter 11, "Configuring storage, security, and analytics for the IBM zAware server," on page 79. |
| | Allow users to browse the operations log (OPERLOG). | Step 6 on page 95 in Chapter 12, "Configuring z/OS monitored clients to send data to the IBM zAware server," on page 91. |
| | Authorize the z/OS system logger to communicate with the IBM zAware server. | Step 3 on page 93 in Chapter 12, "Configuring z/OS monitored clients to send data to the IBM zAware server," on page 91. |

Chapter 7. Planning to use the IBM zAware GUI

Through the IBM zAware graphical user interface (GUI), you can view analytical data that indicates which system is experiencing deviations in behavior, when these anomalies occurred, and details about unusual messages and unusual message patterns. Using this information, you can take corrective action for these anomalies before they develop into more visible problems.

The GUI also provides pages through which you can accomplish additional tasks, which include:

- Checking the status of monitored clients that are connected to the IBM zAware server.
- Modifying the IBM zAware models for monitored clients.
- Configuring storage, security, and analytics controls for the server.

Browser prerequisites

- | To take full advantage of the IBM zAware GUI, you must use one of the following browsers. Edit your browser options to enable JavaScript, Cascading Style Sheets (CSS) and cookies, and to disable software that blocks pop-up windows, especially if you are using keyboard controls rather than the mouse to use the GUI.
- | • Mozilla Firefox Extended Support Release (ESR) 17
- | • Microsoft Windows Internet Explorer 9, with compatibility mode disabled
- | Other browsers and browser release levels might work but have not been tested; if you use them, some IBM zAware functions might not be available and page content might not display correctly.

Network connections

As noted in “Planning network connections and capacity” on page 29, the most logical network option for browser access to the IBM zAware server is an Open Systems Adapter (OSA) channel for a customer-provided data network. This OSA channel path is defined to the IBM zAware partition on which the server runs. For users to access the IBM zAware GUI using this network channel path, port 80 (HTTP) and port 443 (HTTPS) must be open for inbound communication from users and outbound communication from the IBM zAware server.

Security considerations

The following list provides a summary of security considerations that are related to the configuration and use of the IBM zAware GUI. Chapter 6, “Planning for security,” on page 51 provides additional details.

- Browser Certificate Authority (CA) certificate
- Master user ID and password
- User authentication for the IBM zAware GUI
- Role-based access to IBM zAware GUI functions
- Browser session timeout setting

Integration with system management products

IBM zAware provides an application programming interface (API) that system management products can use to request analytical data to display through their own graphic user interfaces. Through this API, system management products, such as IBM Tivoli® OMEGAMON®, can request and receive IBM zAware analytical data in XML format. This data is equivalent to the information that is available through the **Analysis** page and **Interval view** in the IBM zAware GUI.

In addition, your installation can configure the z/OS Management Facility (z/OSMF) so that users can launch the IBM zAware GUI from the z/OSMF **Links** page.

For additional details, see Chapter 22, “Enabling system management products to use IBM zAware data,” on page 191.

| **Accessibility features for the IBM zAware GUI**

| Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully. IBM strives to provide products with usable access for everyone, regardless of age or ability.

| The following list includes the major accessibility features in the IBM zAware GUI:

- | • Keyboard-only operation
- | • Interfaces that are commonly used by screen readers

| **Keyboard navigation**

| This product uses standard operating system navigation keys. You can use keys or key combinations to perform operations and initiate menu actions that can also be done through mouse actions. You can navigate the IBM zAware GUI from the keyboard by using the shortcut keys for your browser or screen-reader software. See your browser or screen-reader software Help for a list of shortcut keys that it supports.

| **Interface information**

| Several pages or display elements in the IBM zAware GUI have more accessible, text-only alternatives:

- | • The tabular view of the Analysis page is provided to improve the accessibility of IBM zAware data. To display the tabular view, click **Switch to Table View** on the toolbar of the Interval Anomaly Scores by System table on the default graphical Analysis page.
- | • The Time Line Summary window provides a text-only format that indicates when a selected message ID was issued during a selected 10-minute interval. To display the text-only format, position your cursor over the graphic display in the Time Line column on the Interval View, and click to open the Time Line Summary window.
- | • The Summary view provides a text-based version of the dates that are associated with a model of system behavior. The Summary view is the default view when you navigate to the **Training Sets > Manage Model Dates** page.

| **IBM and accessibility**

| See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Chapter 8. Planning to create IBM zAware models

To provide analytical data for a monitored client, the IBM zAware server requires a model of normal system behavior to use for comparison. IBM zAware builds a model for each monitored client with message data from that client. You have two options for building a model: waiting for the server to build a model from data collected over a specific time period, or priming the server with prior data. This priming option is recommended because analysis can start shortly after the model is built. Regardless of the option that you choose, you must provide sufficient data for the IBM zAware server to successfully build a model.

Message data requirements for building a model

IBM zAware requires sufficient message data to determine what constitutes normal behavior for a given monitored client. When processing message data from a system, the IBM zAware server determines which messages are issued during routine system events, such as starting a batch job or a particular subsystem. For such system events, the server identifies and recognizes the pattern of messages that are associated with each event. The message patterns are called *clusters* and define the normal context for the messages in the cluster. If the IBM zAware server does not receive a sufficient amount of data for a given system, it is not able to detect and recognize these message clusters.

For a z/OS production system, which is typically a very stable system that produces high-volume, consistent message traffic, IBM zAware can build a model that uses the system's standard behavior as the desired behavior. For less stable systems, such as test systems or development sandbox environments, modelling standard behavior can be more difficult. By default, 90 consecutive calendar days of message data is required for IBM zAware to learn and model the behavior of a given system. This default value, which is known as the *training period* for IBM zAware analytics, covers multiple unusual but predictable events, such as end-of-the-month processing.

Your installation can modify the training period, based on your knowledge of the workloads running on z/OS monitored clients. If you change this value, make sure that the new training period is long enough to include several occurrences of normal events for all systems that you plan to connect to the IBM zAware server. This training period applies for all monitored clients; you cannot define a different training period for each client.

Within the training period, the message traffic for the system must contain a minimum of 375 unique message IDs. Each of those unique IDs must be issued at least once in three different 10-minute intervals during the training period. IBM zAware recognizes messages IDs that conform to the z/OS standard, which consists of a component identifier, a message number, and an action code, in that order. IBM zAware also is capable of recognizing message IDs that do not completely conform to this z/OS standard. Because of this capability, the total count of unique message IDs for a monitored client can consist of messages issued by IBM products, non-IBM products, and possibly your own application programs.

Using the IBM message analysis program is perhaps the easiest way to analyze the message traffic for a given z/OS monitored client. Through this program, you can analyze z/OS SYSLOG data sets to determine the message rate per second, as well as the number and frequency of unique message IDs. The message analysis program is available on the z/OS Tools and Toys web site at the following URL:

<http://www-03.ibm.com/systems/z/os/zos/features/unix/bpxalty2.html>

To find the message analysis program, search the table of download packages for the MSGLG610 package.

The IBM Redbooks publication *Extending z/OS System Management Functions with IBM zAware*, SG24-8070, describes how to use the message analysis program. This Redbooks publication is available at the following URL:

| <http://www.redbooks.ibm.com/>

After you determine the training period that you need for your z/OS systems, you can choose which option to use for training IBM zAware:

- “Option 1: Waiting for the server to build a model,” which uses current OPERLOG data for the model.
- “Option 2: Transferring priming data to build a model,” which uses prior SYSLOG data for the model.

If you recently converted your z/OS system to use OPERLOG, which is a requirement for IBM zAware monitored clients, and that z/OS system was formerly configured or still uses the JES3 DLOG for its hardcopy log, you must use option 1 because option 2 requires SYSLOG data in a specific format. You can use the SYSLOG data on JES2 systems to prime the server but you cannot use SYSLOG data in the JES3 DLOG format for priming.

Option 1: Waiting for the server to build a model

| When you wait for the server to build a model, the training period determines when analytical data will
| be available for a monitored client. The *training period* is the number of consecutive calendar days that the
| IBM zAware server uses to identify the instrumentation data to include in training models. By default,
| the training period is 90 days.

When you wait for the server to build a model, you have to connect the monitored client and make sure that it sends message data to the IBM zAware server for the duration of the training period. The monitored client must meet operating system and configuration requirements to send its OPERLOG data to the server.

| When the training period ends, IBM zAware server automatically attempts to create the initial model for
| the monitored client. If the automatic build of the initial model is successful, IBM zAware can begin to
| analyze current data that it receives from the client. From this point on, IBM zAware uses the training
| interval value to determine when to automatically rebuild the system model. The *training interval* is the
| number of consecutive calendar days between automatic builds of system behavior models. By default,
| the training interval is 30 days.

Until a model is successfully built, the server is not able to provide analytical data. In this case, when you view the **Analysis** page in the IBM zAware graphical user interface (GUI), the monitored client is listed in the page display but no anomaly scores are provided for this client. To verify that the client is connected and sending data, use the **System Status** page in the GUI.

Option 2: Transferring priming data to build a model

Instead of waiting for the IBM zAware server to collect data over the course of the training period, you can prime the server by transferring prior data from the hardcopy or system logs of monitored clients, and requesting the server to build a model for each client from the transferred data.

The priming process consists of several phases:

1. The transfer of prior data to the IBM zAware server. To transfer this priming data, you configure a log stream and run the z/OS bulk load client for IBM zAware through a REXX exec on a z/OS system.

The process of transferring priming data could require several hours or more, depending on a number of factors that include:

- The priority of the job that runs the REXX EXEC for the z/OS bulk load client
- The amount of priming data to be sent, and whether any of that priming data resides on migrated data sets

- The network configuration and traffic at your installation

For example, if you run the REXX EXEC at a very high priority to send 46000 tracks of priming data that is archived, the transfer might take approximately 10 to 15 minutes. The process can take longer if the z/OS bulk load client runs at a lower priority, or if network or system conditions are not favorable when the REXX EXEC runs.

2. The assignment of priming data to the correct sysplex.

In contrast to data that the IBM zAware server receives from the z/OS system logger running on a monitored client, the priming data from the z/OS bulk load client does not include the name of the sysplex to which the monitored client belongs. Without the sysplex name, the IBM zAware server cannot associate the priming data with the appropriate sysplex. You use the **Administration > Configuration > Priming Data** page in the IBM zAware GUI to assign the received priming data to the appropriate sysplex. After the priming data is associated with the appropriate sysplex, you can request the IBM zAware server to build the model.

3. The training of the IBM zAware server, which results in a model of normal system behavior.

To build the model for a specific monitored client, you have two options:

- You can use the **Request Training** action on the **Administration > Training Sets** page. Any data that the z/OS system logger is currently sending does not become part of the model for the client until you request training again or the IBM zAware server automatically rebuilds the model. This priming option is recommended because analysis can start shortly after the model is built.
- You can wait for the next scheduled training, during which the IBM zAware server automatically uses the priming data to build the model. In this case, any data that the z/OS system logger is currently sending becomes part of the model for the client.

Note that analytical data is not available for the dates for which you supplied priming data, unless the monitored client was connected and sending data to the IBM zAware server on those dates. The server does not analyze priming data; it uses priming data only for creating the model of system behavior.

Through the z/OS bulk load client, you can transfer data for one or more monitored clients by identifying the sequential data sets that contain the priming data. The sequential data sets can contain only SYSLOG data that is stored in hardcopy log 2-digit year (HCL) or 4-digit year (HCR) format. If any data set has been archived, the z/OS bulk load client can recall the data set, transfer its contents, and migrate the data set.

The recommended approach to priming is to complete the following tasks in sequence.

1. Configure a Quality Assurance (QA) system as a IBM zAware monitored client. Use the instructions in Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91.
2. From the QA system, run the z/OS bulk load client to send priming data and build models for all the systems that you want to configure as monitored clients.
 - a. Transfer only a portion of the priming data for a monoplex or sysplex to validate the configuration of the IBM zAware environment.
 - b. When you verify that the transfer was successful, transfer the remaining data for one monoplex or sysplex at a time. If you transfer priming data for multiple sysplexes through one invocation of the REXX exec, priming data for some systems can be overlaid.

To send priming data and build models, use the instructions in Chapter 13, “Creating an IBM zAware model for new z/OS monitored clients,” on page 99.

3. Configure the systems for which you transferred priming data as IBM zAware clients.

Although the primary use of the z/OS bulk load client is to quickly build the initial model for a monitored client, you can use it after initial setup as well. For example, if a monitored client is disconnected from the IBM zAware server for an extended period of time, and you believe that the message traffic generated on that system during that time is important to include in the system model, you can use the z/OS bulk load client to transfer that generated message data. Remember, however, the

server does not analyze priming data, so analytical data is not available for the time period during which the monitored client was disconnected. Also, the process of assigning priming data results in automatic recycling of the analytics engine and the disconnection of all monitored clients, so you need to determine whether the missing message data is worth this disruption to your IBM zAware environment.

Part 3. Configuring IBM zAware and its monitored clients

Topics in this part provide step-by-step instructions for configuring the IBM zAware environment, which includes the IBM zAware partition, the IBM zAware server, and its monitored clients. Systems programmers and administrators use these configuration tasks primarily for first-time setup.

Topics covered in this part are:

- Chapter 9, “Configuring network connections and storage for the IBM zAware partition,” on page 63
- Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67
- Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79
- Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91
- Chapter 13, “Creating an IBM zAware model for new z/OS monitored clients,” on page 99

Chapter 9. Configuring network connections and storage for the IBM zAware partition

Use this procedure to learn how to configure network connections and persistent storage for the IBM zAware partition. This procedure is intended for experienced system programmers, network administrators, or storage administrators who are responsible for configuring a zEC12 or zBC12 central processor complex (CPC) and its peripheral hardware devices.

Before you begin

For optimal performance and operations, configure the IBM zAware partition such that it has access to only those channel path identifiers (CHPIDs), control units, and I/O devices that are required for network connectivity and storage.

- Your installation must have correctly installed and configured a zEC12 or zBC12 CPC on which you can configure the IBM zAware partition. Planning information and instructions for installing, configuring, and activating a zEC12 are available in the following:
 - *zEnterprise EC12 System Overview*, SA22-1088 or *zEnterprise BC12 System Overview*, SA22-1089
 - *zEnterprise EC12 Installation Manual*, GC28-6913 or *zEnterprise BC12 Installation Manual*, GC28-6913
 - The **System z HMC and SE (Version 2.12.1) Information Center** at <http://pic.dhe.ibm.com/infocenter/hwmca/v2r12m1/index.jsp>
- To complete most of the configuration tasks in this procedure, you use either the Hardware Configuration Definition (HCD) or the Input/Output Configuration Program (IOCP). Depending on the tool you are using, you might need to see one of the following books:
 - *z/OS Hardware Configuration Definition User's Guide*, SC33-7988, and *z/OS Hardware Configuration Definition Scenarios*, SC33-7987
 - *System z Input/Output Configuration Program User's Guide for ICP IOCP*, SB10-7037
- Make sure that you have reviewed the network planning considerations in “Planning network connections and capacity” on page 29, and have acquired the appropriate resources. Peripheral devices for network connections must be installed and attached to the zEC12 or zBC12 before you begin this procedure.
- Make sure that you have reviewed the storage planning considerations in “Planning persistent storage configuration and capacity” on page 35, and have acquired the appropriate resources. Peripheral devices for storage must be installed and attached to the zEC12 or zBC12 before you begin this procedure.

Attention: To avoid the potential loss of critical system and application data on storage devices connected to the CPC, the storage administrator must use either channel path definition lists or the explicit candidate device list in HCD to ensure that only the IBM zAware partition can access the devices that are intended for IBM zAware use. The only exception to this practice is the CPC partition, if any, that your installation is using to back up the storage that the IBM zAware server is using.

About this task

Through either HCD or the IOCP, you can define network connections and storage devices for the IBM zAware partition in the input/output configuration data set (IOCDS) for the zEC12 or zBC12 CPC. HCD supplies an interactive dialog to generate the I/O definition file (IODF) and subsequently the IOCDS, whereas IOCP generates the IOCDS without the use of an IODF. Using HCD is preferred for generating the I/O configuration because HCD performs validation checking as you enter data, which helps minimize the risk of errors. The information in this procedure is tailored for HCD users.

The steps in this procedure provide the information that you need to update the IOCDS for the IBM zAware partition. Additional network and storage configuration tasks are required to complete the initial setup for the IBM zAware environment; these tasks are documented in the following topics:

- Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67
- Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79
- Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91

Procedure

1. Through HCD, add the IBM zAware partition to the I/O configuration for the host system (zEC12 or zBC12 CPC).

- a. Add the IBM zAware partition to the list of partitions for the host system.

- The name that you provide for the partition must exactly match the name that you use for the LPAR image profile that you create in Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67.
- The partition usage field marks a partition to be used for coupling facility support or for operating system usage. For partition usage, enter OS for operating system.

- b. Define or update channel path definitions for the IBM zAware host system.

The recommended practice is to configure the IBM zAware partition such that it has access to only those channel path identifiers (IDs), control units, and I/O devices that are required for network connectivity and storage. When defining storage devices in the IODF or IOCDS for the IBM zAware host system, the network administrator can use the following HCD constructs to limit IBM zAware access to specific resources.

- Image access and candidate lists in channel path definitions
- The explicit device candidate list for I/O devices

- 1) Assign channel paths to the IBM zAware partition for network connections. Table 16 lists the types of channel paths that you can assign.

Table 16. Supported channel path types for the IBM zAware partition

| Channel path type | Description | IBM zAware usage | Additional information |
|-------------------|---|---|--|
| OSD | Ethernet connectivity through an Open Systems Adapter (OSA) channel | <ul style="list-style-type: none"> • Use for monitored clients that reside on any supported System z CPC in the IBM zAware environment. • Use for GUI browser connections to the IBM zAware server. | <i>zEnterprise System, System z10, System z9 and eServer zSeries Open Systems Adapter-Express Customer's Guide and Reference, SA22-7935</i> Note: For OSA-Express3 or later generation features, IBM zAware can use only port 0. |
| OSX | Connectivity through the intraensemble data network (IEDN) | Use only for monitored clients that reside on the IBM zAware host system or on other nodes in the same zEnterprise ensemble. | |
| IQD | Connectivity through HiperSockets | Use only for monitored clients that reside on the IBM zAware host system. Use the IQD channel path type for HiperSockets over the IEDN. | <i>z/OS Communications Server: IP Configuration Guide, SC31-8775</i> |

- 2) If necessary, change the channel path mode. Channel paths can be dedicated, reconfigurable, shared, or spanned.

DED Dedicated; if you want only one logical partition to access a channel path, specify that channel path as dedicated. You cannot reconfigure a dedicated channel path. This is the default mode.

REC Reconfigurable; if you want only one logical partition at a time to access a channel path and you want to be able to reconfigure the channel path from one partition to another, specify that channel path as reconfigurable.

SHR Shared; if you want more than one logical partition to access a channel path simultaneously, specify that channel path as shared.

SPAN

Spanned; if in XMP processors for certain channel types, you want to have a shared channel accessed by partitions from multiple logical channel subsystems, specify that channel path as spanned.

- c. Add the IBM zAware partition to the access list for each channel path that you have selected.
- d. Verify your configuration changes. One way to verify your changes is to build an IOCP input data set and view it to check the partition list for the channel path that you have defined.

As an alternative, you can view your changes graphically if your system meets the appropriate HCD prerequisites. On the HCD Channel Path List panel:

- 1) Select the channel paths and press **Enter**.
- 2) Select **View graphically** and press **Enter**.

2. Configure persistent storage for the IBM zAware partition.

- When defining storage devices in the IODF or IOCDS for the IBM zAware host system, the storage administrator can use image access and candidate lists for channel path definitions to allow only the IBM zAware partition to access specific devices. Using the explicit device candidate list is an alternative method of restricting access to specific devices.
- As an additional precaution, you can use channel path definition lists, the explicit device candidate list, or operating system mechanisms to prevent the applications running in other CPC partitions from using storage devices that are intended for IBM zAware use.

The only exception to this practice is the CPC partition, if any, that your installation is using to back up the storage that the IBM zAware server is using.

The IBM zAware partition uses direct access storage devices (DASD) that are attached to the host system. For DASD storage only, complete the following general steps.

- a. On the storage controller, define volumes.
- b. Through HCD, complete the following steps:
 - 1) Define the channel path for the storage device. Add the IBM zAware partition to the access list for the channel paths for the storage devices.
 - 2) Define the control unit (controller).
 - 3) Define the storage device, using the explicit candidate list as appropriate for your planned IBM zAware environment.

3. Verify your configuration changes. One way to verify your changes is to build an IOCP input data set and view it to check the partition list for the channel path that you have defined.

As an alternative, you can view your changes graphically if your system meets the appropriate HCD prerequisites. On the HCD Channel Path List panel:

- a. Select the channel paths and press **Enter**.
- b. Select **View graphically** and press **Enter**.

Results

Network connections and persistent storage are configured for the IBM zAware partition.

What to do next

Activate your configuration according to your company operating procedures. Depending on your environment, you might be able to dynamically update the IODF; another option is to complete the following steps.

1. Through HCD:
 - a. Build a production IODF.
 - b. Build an IOCDS.
2. Through the HMC:

- | a. Perform power on reset (POR) for the IBM zAware host system, with the new IOCDS.
- | b. Define the new partition as instructed in Chapter 10, “Configuring an image profile for the IBM
- | zAware partition,” on page 67.

Chapter 10. Configuring an image profile for the IBM zAware partition

Use this procedure to configure the logical partition (LPAR) that is dedicated to running an instance of IBM zAware. This procedure is intended for experienced system programmers who are responsible for configuring logical partitions on a zEnterprise System central processor complex (CPC). Depending on the IT roles and responsibilities at your installation, you might need to collaborate with network administrators to complete specific configuration tasks.

Before you begin

- Your installation must have correctly installed and configured a zEC12 or zBC12 on which you can configure the IBM zAware partition. Planning information and instructions for installing, configuring, and activating a zEC12 or zBC12 are available in the following:
 - *zEnterprise EC12 System Overview*, SA22-1088 or *zEnterprise BC12 System Overview*, SA22-1089
 - *zEnterprise EC12 Installation Manual*, GC28-6913 or *zEnterprise BC12 Installation Manual*, GC28-6913
 - The **System z HMC and SE (Version 2.12.1) Information Center** at <http://pic.dhe.ibm.com/infocenter/hwmca/v2r12m1/index.jsp>
- Before you can create an image profile for the IBM zAware partition, make sure that the CPC reset profile for the zEC12 specifies the activation order for the new IBM zAware partition.
- Before activating the IBM zAware partition, make sure that I/O and storage devices have been configured for this partition. Use the instructions in Chapter 9, “Configuring network connections and storage for the IBM zAware partition,” on page 63.

The image profile name for the IBM zAware partition must be the same as the name of an LPAR image in the input/output configuration data set (IOCDS) for the zEC12 or zBC12 CPC. Otherwise, the IBM zAware partition cannot be activated.

- To prepare to use the Hardware Management Console (HMC) to configure the IBM zAware partition, make sure that you:
 - Know the name of the LPAR image that you plan to configure as the IBM zAware partition. The names of LPAR images are listed in the I/O definition file (IODF) for the zEC12 or zBC12 CPC. The name of the image profile that you customize through the HMC must be the same as the LPAR image name in the IODF.
 - Review the planning considerations for an IBM zAware partition in *zEnterprise System PR/SM Planning Guide*, SB10-7156.
 - Log in to the HMC with a user ID that is assigned to the system programmer role (SYSPROG).

About this task

This procedure provides instructions for creating a customized image profile for the LPAR that is dedicated to running IBM zAware. You use an image profile to activate a logical partition.

Through the HMC, you select either the default image profile or an existing image profile for an LPAR on the zEC12 or zBC12 CPC that serves as the IBM zAware host system. Alternatively, you can select an existing image profile and use it as a model to create a new image profile. If you select the default image profile or create a new image profile based on an existing profile, you must replace the profile name with a name that is the same as the name of an LPAR image in the IOCDS or IODF for the zEC12 or zBC12 CPC.

The mode that you specify in the image profile defines the LPAR as an IBM zAware partition. When you select **zAware** as the partition mode, the HMC adjusts the navigation pane and individual page content to display page links and LPAR characteristics that are appropriate for an IBM zAware partition. This

procedure provides information primarily for LPAR characteristics that are unique to an IBM zAware partition. If you need additional information about other LPAR characteristics that you can specify, see the HMC online help.

Procedure

1. Through the HMC, select the IBM zAware host system (zEC12 or zBC12 CPC) and start the **Customize/Delete Activation Profiles** task. Select the LPAR that is to function as the IBM zAware partition and either create or customize its image profile.
Make sure that you select an LPAR that is associated with the IBM zAware host system (zEC12 CPC). Figure 21 shows the list of profiles associated with a zEC12 CPC named “P92”. This list of profiles is populated from LPAR definitions in the IOCDs or IODF for the “P92” CPC. An image named “ZAWARE1”, for which the image profile has not been created, is selected.
The remaining steps and figures in this procedure illustrate how to customize an existing image

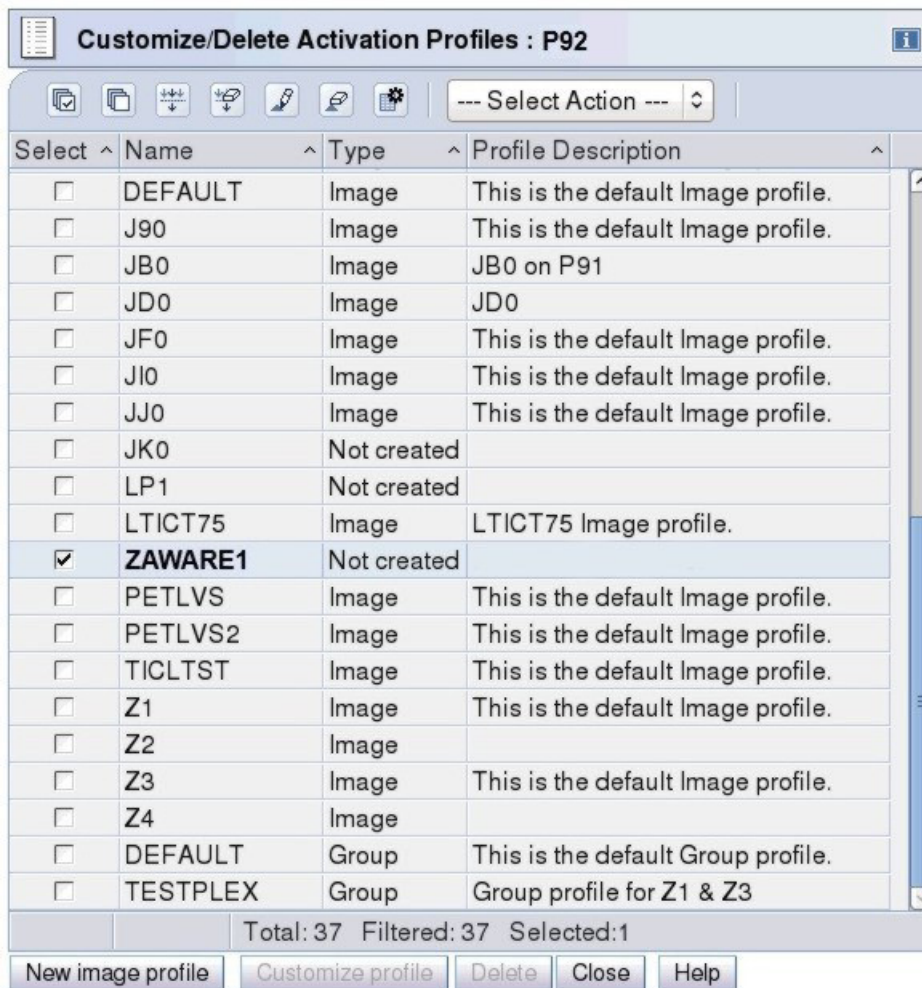


Figure 21. LPAR image profile: Selecting the name of the IBM zAware partition to create a new image profile

profile for a partition named “ZAWARE1”; however, you can use this information to help you create an image profile through the New image profile wizard.

2. On the Customize Image Profiles window, select the **General** page from the profile tree view to define the partition mode and other characteristics. Select **zAware** mode to define this LPAR as the IBM zAware partition. Figure 22 on page 69 shows sample values for the **General** page.
 - a. If you are using the default image profile or an existing image profile as a template for a new image profile, or you selected the default image profile, supply a new name for this image profile by typing over the displayed name before you make any other changes, and click **Save** to save the

profile with the new name. The image profile name for the IBM zAware partition must be the same as the name of an LPAR image in the IOCDS or IODF for the zEC12 or zBC12 CPC. See Table 17 for additional details about profile names.

- b. For **Mode**, select the **zAware** mode from the scrollable list. When you select **zAware** as the partition mode, the HMC adjusts the navigation pane and individual page content to display LPAR characteristics that are appropriate for an IBM zAware partition. For example, Figure 22 shows the **zAware** page tab in the navigation pane.

Figure 22. LPAR image profile: General characteristics with the IBM zAware mode

Table 17 describes the LPAR characteristics that you can specify on this page and the values that are required for the IBM zAware partition.

Table 17. Image profile: zAware partition values for the General page

| LPAR characteristic | Value to supply for IBM zAware partition |
|---------------------|--|
| Profile name | <p>If you select the default image profile, enter a new name for the IBM zAware partition. The image profile name for the IBM zAware partition must be the same as the name of an LPAR image in the IOCDS or IODF for the zEC12 or zBC12 CPC.</p> <p>Attention: Because configuration information about the IBM zAware environment is associated with the partition name that you provide, do not rename this partition after you have activated it and have configured the IBM zAware server and its clients.</p> <p>A profile name can be from 1 to 8 characters long. It cannot have special characters or imbedded blanks. Valid characters for a profile name are:</p> <p>Characters 0 through 9 Decimal digits</p> <p>Characters A through Z Letters of the English alphabet</p> <p>Profile names are not case-sensitive. All alphabetic characters are saved in uppercase.</p> |

Table 17. Image profile: zAware partition values for the General page (continued)

| LPAR characteristic | Value to supply for IBM zAware partition |
|-----------------------|--|
| Description | Enter a brief description for the IBM zAware partition. |
| Partition identifier | Specify two hexadecimal digits to identify the IBM zAware partition. The partition identifier can be from X'0' to X'3F'. |
| Mode | Select the zAware mode from the scrollable list. |
| Clock Type Assignment | Select Standard time of day to set the LPAR clock to the same time set for the zEC12 time source. |
| LICCC configuration | Make sure that a check mark is displayed to ensure that the image profile data conforms to the current maximum Licensed Internal Code Configuration Control (LICCC) configuration. |

3. Select the **Processor** page in the profile tree view to assign processors for the IBM zAware partition. Figure 23 shows sample values for the **Processor** page.

Customize Image Profiles: P92:ZAWARE1 : ZAWARE1 : Processor

Group Name: <Not Assigned>

Logical Processor Assignment

- ☐ Dedicated central processors
- ☐ Dedicated integrated facility for Linux
- ☐ Not dedicated central processors
- ☒ Not dedicated integrated facility for Linux

Not Dedicated Processor Details

Initial processing weight: 500 (1 to 999) ☒ Initial capping

Number of processors - Initial: 2 Reserved: 0

Buttons: Cancel, Save, Copy Profile, Paste Profile, Assign Profile, Help

Figure 23. LPAR image profile: Processor characteristics

Table 18 on page 71 describes the LPAR characteristics that you can specify on this page and the values that are required for the IBM zAware partition.

Table 18. Image profile: IBM zAware partition values for the Processor page

| LPAR characteristic | Value to supply for IBM zAware partition |
|---------------------------------|--|
| Group name | If you choose to assign the processor to a group, select a defined group from the list or enter the name of a group that you plan to define at a later time. |
| Logical Processor Assignment | <p>For the IBM zAware partition, you can select one of the following choices. The use of IFLs is preferable, especially for dedicated use, because IFLs are less costly than central processors.</p> <p>Dedicated central processors Select this option if you want a central processor dedicated to each logical processor.</p> <p>Dedicated integrated facilities for Linux If integrated facilities for Linux (IFL) is supported and installed in the zEC12 or zBC12 CPC, select this option if you want an integrated facilities for Linux dedicated to each logical processor.</p> <p>Not dedicated central processors Select this option if you want the logical processors to share central processors that are not already dedicated to other activated logical partitions when this partition is activated.</p> <p>Not dedicated integrated facilities for Linux Select this option if you want the logical processors to share IFL processors that are not already dedicated to other activated logical partitions when this partition is activated.</p> |
| Not Dedicated Processor Details | <p>If you select “Not dedicated” processors, provide values in the Initial processing weight and Initial capping fields.</p> <p>Initial processing weight Specify the partition processing weight for sharing the not dedicated processors. The processing weight can be from 1 to 999.</p> <p>Initial capping Specify whether the logical partition is prevented from using the not dedicated processors in excess of its processing weight. To indicate the logical partition cannot use the not dedicated processors in excess of its processing weight, select this option.</p> |

Table 18. Image profile: IBM zAware partition values for the Processor page (continued)

| LPAR characteristic | Value to supply for IBM zAware partition |
|----------------------|---|
| Number of processors | <p>Provide the number of initial or reserved processors.</p> <p>Initial The number of initial processors that you need to specify depends on the amount of data that monitored clients send to IBM zAware for processing.</p> <p>Reserved Specify the number of reserved processors that you want assigned to the IBM zAware partition.</p> <p>Use the following guidelines to determine the amount of processor resource your installation requires. These guidelines are based on IBM testing of the two operations phases: initial priming and training, and analysis. Keep in mind that IFLs run at full capacity, but CPs can run at full capacity or various subcapacity settings, depending on the zEC12 or zBC12 model. These guidelines are based on IFLs or CPs that are running at full capacity.</p> <p>For an IBM zAware partition on a zEC12</p> <ul style="list-style-type: none"> For configurations with up to 10 monitored clients, for a total maximum rate of 500 messages per second: <ul style="list-style-type: none"> Approximately 25% of one zEC12 IFL or 25% of one full-capacity zEC12 CP (for example, model 701) is required for initial priming and training. Approximately 20% of one zEC12 IFL or 20% of one full-capacity zEC12 CP (for example, model 701) is required for analysis operations. For configurations with up to 10 monitored clients, for a total maximum rate of 1500 messages per second: <ul style="list-style-type: none"> Approximately 80% of one zEC12 IFL or 80% of one full-capacity zEC12 CP (for example, model 701) is required for initial priming and training. Approximately 40% of one zEC12 IFL or 40% of one full-capacity zEC12 CP (for example, model 701) is required for analysis operations. <p>If you connect more than 10 monitored images during a 15-minute interval when the maximum message rate per second is approximately 1500, the capacity of a single zEC12 IFL or a single full-capacity zEC12 CP might be overrun during the initial priming and training phase. To avoid this potential condition, you can configure a second zEC12 IFL or CP for IBM zAware to use.</p> <p>For an IBM zAware partition on a zBC12</p> <ul style="list-style-type: none"> For configurations with up to 10 monitored clients, for a total maximum rate of 500 messages per second: <ul style="list-style-type: none"> Approximately 30% of one zBC12 IFL or 30% of one full-capacity zBC12 CP (for example, model z01) is required for initial priming and training. Approximately 20% of one zBC12 IFL or 20% of one full-capacity zBC12 CP (for example, model z01) is required for analysis operations. For configurations with up to 10 monitored clients, for a total maximum rate of 1500 messages per second: <ul style="list-style-type: none"> Approximately 95% of one zBC12 IFL or 95% of one full-capacity zBC12 CP (for example, model z01) is required for initial priming and training. Approximately 40% of one zBC12 IFL or 40% of one full-capacity zBC12 CP (for example, model z01) is required for analysis operations. <p>If you connect more than 10 monitored images during a 15-minute interval when the maximum message rate per second is approximately 1500, the capacity of a single zBC12 IFL or CP might be overrun during the initial priming and training phase. To avoid this potential condition, you can configure a second zBC12 IFL or CP for IBM zAware to use.</p> |

4. Select the **Security** page in the profile tree view to define the security characteristics for the IBM zAware partition. Figure 24 shows sample values for the **Security** page.

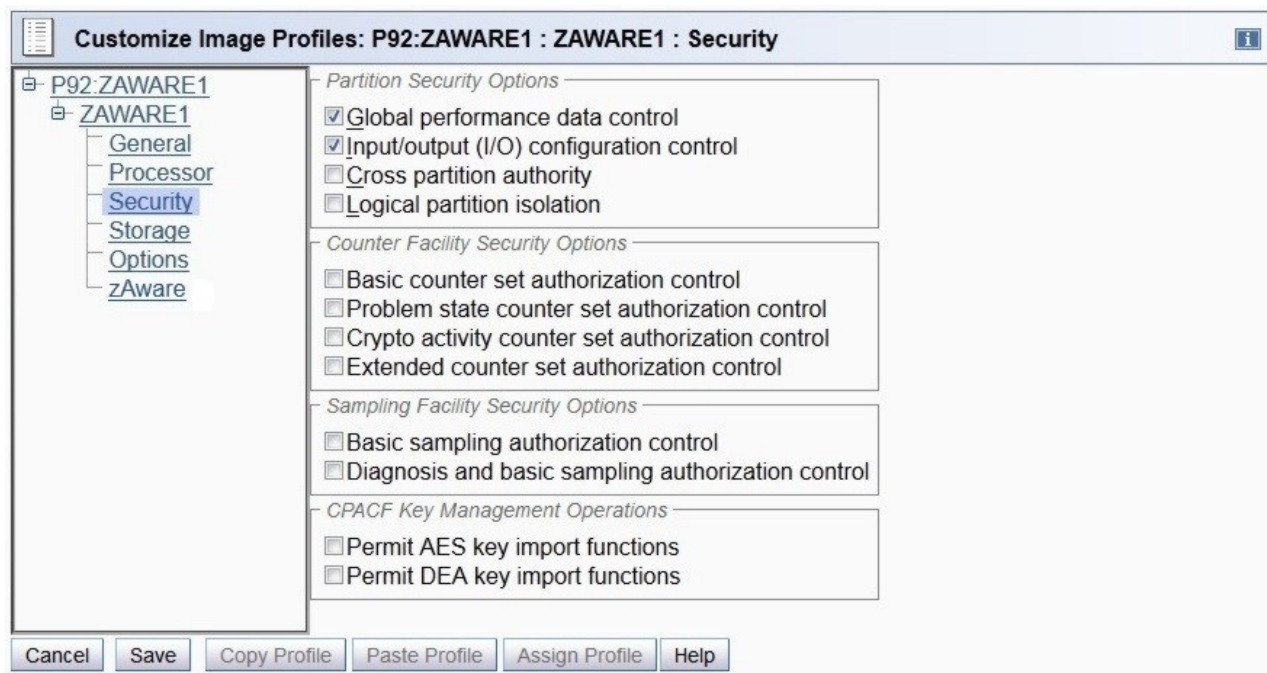


Figure 24. LPAR image profile: Security characteristics

Table 19 describes the LPAR characteristics that you can specify on this page and the values that are required for the IBM zAware partition.

Table 19. Image profile: IBM zAware partition values for the Security page

| LPAR characteristic | Value to supply for IBM zAware partition |
|------------------------------------|---|
| Partition Security Options | You can select any of the partition security options. |
| Counter Facility Security Options | IBM zAware does not make use of the counter facility so these options do not apply. |
| Sampling Facility Security Options | IBM zAware does not make use of the sampling facility so these options do not apply. |
| CPACF Key Management Options | Cryptographic functions cannot be specified for the IBM zAware partition so these options do not apply. |

5. Select the **Storage** page in the profile tree view to define the storage characteristics for the IBM zAware partition. IBM zAware uses only central storage, not expanded storage. Figure 25 on page 74 shows sample values for the **Storage** page.

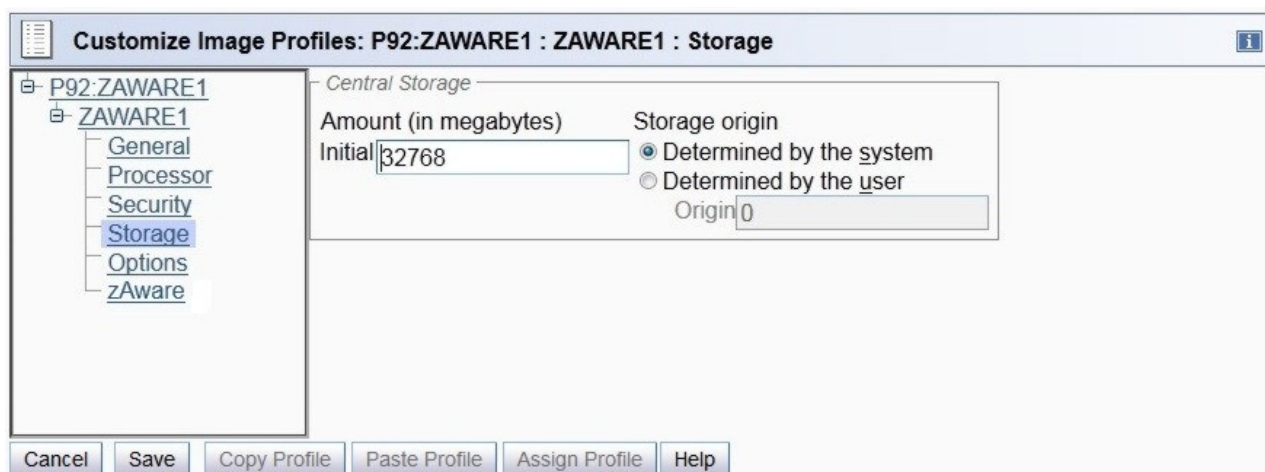


Figure 25. LPAR image profile: Storage

Specify central storage values for the IBM zAware partition:

Amount (in megabytes)

Central storage is the amount of storage, in megabytes (MB), that is available to allocate for main storage.

Initial Enter the amount of central storage to allocate to the IBM zAware partition on activation.

- You must allocate a minimum of 4096 MB (4 GB) to activate the IBM zAware partition. This amount of memory is sufficient to support a relatively small number of monitored clients (six or fewer) with relatively light message traffic (500 messages per second).
- If your installation plans to connect more than six monitored clients, you need to assign an additional 256 MB of memory for each monitored client. Use the following formula for determining the amount of memory to assign to the partition.

$$4096\text{MB} + (256\text{MB} * (\text{number of clients}))$$

Storage origin

Use these selections to indicate how the central storage origin is determined.

Determined by the system

To have the CPC determine the central storage origin, select this option.

Determined by the user

To have this profile set the central storage origin, select this option, then specify the origin in the **Origin** field.

Origin

If you select to have this profile set the central storage origin, enter the origin. The origin is an offset, not an address. Enter the number of megabytes offset from where available CPC central storage begins, to where you want logical partition central storage to begin.

6. Select the **Options** page in the profile tree view to define the image options for the IBM zAware partition. Figure 26 on page 75 shows sample values for the **Options** page.

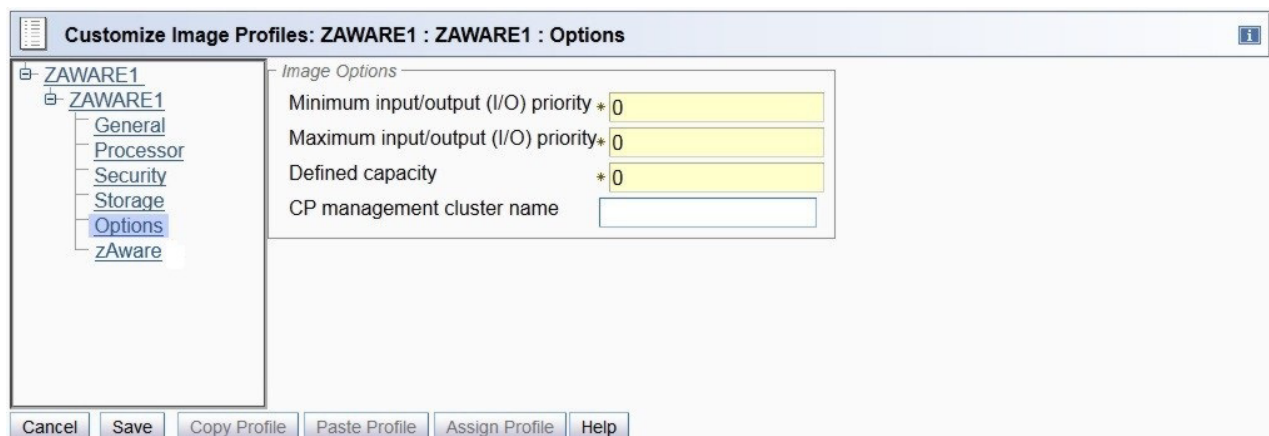


Figure 26. LPAR image profile: Options

Specify values for the IBM zAware partition:

Minimum input/output (I/O) priority

Enter the minimum priority to be assigned to I/O requests from this logical partition.

Maximum input/output (I/O) priority

Enter the maximum priority to be assigned to I/O requests from this logical partition.

Defined capacity

Enter the upper bound in terms of millions of service units (MSUs) beyond which the rolling 4-hour average CPU utilization cannot exceed.

CP management cluster name

Do not enter a cluster name for the IBM zAware partition.

7. Select the **zAware** page in the profile tree view to define network settings for the IBM zAware partition and assign the default master user ID and password for accessing the IBM zAware graphical user interface (GUI). Figure 28 on page 77 shows sample content for a **zAware** page.
 - a. Provide values for the host name, default master user ID, and password.

Host name

Enter the host name for the IBM zAware partition. To use the IBM zAware GUI, users need to specify a URL that contains either a host name or an IP address for the partition.

A host name can be from 1 through 32 characters long. It cannot contain imbedded blanks. Valid characters are numbers 0 through 9, letters A through Z (upper or lower case), and the following special characters: period (.), colon (:), and hyphen (-).

Master user ID

Enter the user ID to be used as the default master user ID for IBM zAware. This user ID has authority to perform any task that is available through the IBM zAware GUI.

A master user ID can be from 1 through 32 characters long. It cannot contain imbedded blanks. Valid characters are numbers 0 through 9, letters A through Z (upper or lower case), and the following special characters: period (.), underscore (_), and hyphen (-).

Master password

Enter the password for the master user ID. A master password can have a minimum of 8 characters and a maximum of 256 characters. A master password is case-sensitive and can contain numbers 0 through 9, letters A through Z (upper or lower case), and the following special characters: hyphen (-), underscore (_), exclamation (!), at (@), hash (#), dollar (\$), percent (%), carat (^), ampersand (&), asterisk (*), left parenthesis ((), right parenthesis ()), plus (+), left brace ({), right brace (}), vertical bar (|), colon (:), less than (<), greater than (>), question mark (?), and equals (=).

Confirm master password

Reenter the password exactly as you typed it for the Master password field.

b. Customize the network adapter configuration for IBM zAware.

- 1) From the **Select Action** list in the Network Adapters table, click **Add/Edit Network Adapters** to define a network connection. The Add/Edit Network Adapters Entry window is displayed.

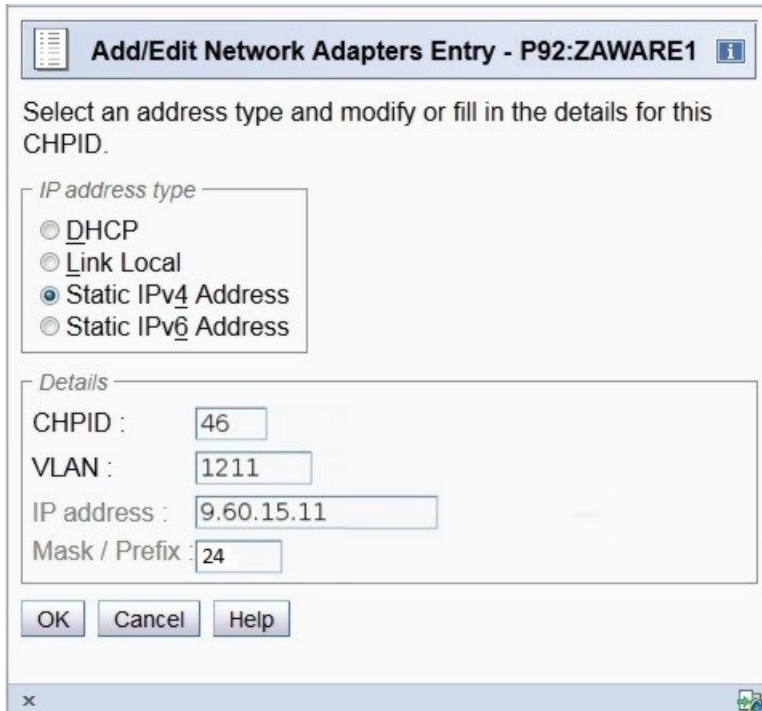


Figure 27. Adding a new network adapter using an IPv4 address

- 2) For each type of network connection in the IBM zAware environment, supply the following information.

For example, if some monitored clients are using a HiperSockets subnet and others are using an Open Systems Adapter (OSA) channel to communicate with the IBM zAware server, you need to define two network adapters: one for the Hipersockets subnet and another for the OSA channel.

IP address type

Select one of the following types:

- Dynamic Host Connection Protocol (DHCP)
- Link local addressing
- Static IPv4 Address
- Static IPv6 Address

The type you select determines which of the remaining fields you can complete; if a field does not apply for a specific selected type, you cannot enter a value.

CHPID

Enter the logical channel path identifier (CHPID) of the network adapter.

VLAN Specify the virtual local area network (VLAN) if the link you are using is defined in TRUNK mode.

IP Address

Enter the IP address of the network adapter. This field is available only for the **Static IPv4 Address** and **Static IPv6 Address** IP address types.

Mask/Prefix

For an IPv4 or IPv6 address, optionally specify the 2-digit mask/prefix. If you need to convert a 4-byte subnet mask to the 2-digit format, you can find several subnet mask converters on the Internet.

- You can define from 1 through 100 connections.
- You can define multiple connections using the same CHPID.
- You can assign both **Static IPv4 Address** and **Static IPv6 Address** IP address types to the same CHPID/VLAN set. To do so requires one connection entry for IPv4 and another connection entry for IPv6.

3) Click **OK** to save your changes and return to the **zAware** page.

c. Customize global network attributes for IBM zAware.

1) In the **Default gateway** field, enter an IPv4 or IPv6 address for the default gateway.

2) From the **Select Action** list in the DNS Servers table, click **Add/Edit DNS server** to define a primary domain name system (DNS) server. The Add/Edit DNS Entry window is displayed. You can define a maximum of two DNS entries.

A DNS server definition is required if you specified a DHCP-type IP address for any of the network adapters for the IBM zAware partition.

3) Enter the IPv4 or IPv6 address of the DNS server.

4) Click **OK** to save your changes and return to the **zAware** page.

Figure 28 shows a **zAware** page that contains some sample values. Note that, for network adapters defined with an IP address type of DHCP, the active IP addresses are displayed along with their associated devices.

Customize Image Profiles: P92:ZWARE1 : ZWARE1 : Firmware

Host name :

Master user ID :

Master password :

Confirm master password :

Network Adapters

| Select ^ | CHPID ^ | VLAN ^ | Requested IP Address/Mask ^ | Active IP Address/Mask ^ | Device Number ^ |
|-----------------------|---------|--------|-----------------------------|---|------------------------------------|
| <input type="radio"/> | AE | 5 | 192.168.4.1/24 | 192.168.4.1/24 | |
| <input type="radio"/> | AE | | 192.168.3.1/24 | 192.168.3.1/24 | |
| <input type="radio"/> | 03 | | DHCP | 192.168.6.2/24, 192.168.6.1/24, fd00::2/127 | 0.0.1530, 0.0.1531, 0.0.1532 |

Default gateway :

DNS Servers

| Select ^ | IP address ^ |
|-----------------------|--------------|
| <input type="radio"/> | 9.12.16.2 |

Buttons: Cancel, Save, Copy Profile, Paste Profile, Assign Profile, Help

Figure 28. LPAR image profile: **zAware** page

8. Click **Save** when you finish working with the image profile for the IBM zAware partition. The HMC displays a message indicating the status of the save operation.

Results

The image profile for the IBM zAware partition is complete.

What to do next

- If you have already completed the procedure in Chapter 9, “Configuring network connections and storage for the IBM zAware partition,” on page 63, you can activate the IBM zAware partition. Do not activate the partition without first defining its I/O and storage in an IODF or IOCDS for the zEC12 or zBC12 CPC, and either switching to the updated IOCDS or dynamically updating it.

The following steps describe one method of activating the partition through the HMC:

1. Select the image for the IBM zAware partition.
2. From the **Daily** task group, open the **Activate** task. The Activate Task Confirmation window is displayed.
3. Review the confirmation text to decide whether to proceed with the task. If you want to continue this task, click **Yes**. The Activate Progress window is displayed indicating the progress of the activation and the outcome.
4. Click **OK** to close the window when the activation completes successfully.

Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

- When the IBM zAware partition is activated, IBM zAware is started automatically. The startup process for IBM zAware might take some time to complete, as its software stack is initialized and configured. When this automatic process completes, the analytics engine is started and the IBM zAware GUI is available for use.

An instance of IBM zAware running on the activated partition is called an IBM zAware server. To prepare the server for operation, complete the procedure in Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79.

- To determine whether the network connection is defined and working correctly, you can ping the IBM zAware server from a z/OS system on the same network. From the TSO command panel or the READY prompt on the z/OS system, enter the **PING** or **TRACERTE** command with either the IP address or host name of the IBM zAware server.

Chapter 11. Configuring storage, security, and analytics for the IBM zAware server

Use this procedure to configure persistent storage, set up security, and configure settings for the analytics engine in the IBM zAware server. Depending on the roles and responsibilities defined for your IT organization, systems programmers, storage administrators, and security administrators might be required to collaborate to complete all of the steps in this procedure.

Before you begin

- The IBM zAware partition must be defined according to the instructions in Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67, and activated.
- You need to know the default master user ID and password and the URL to access and log in to the IBM zAware graphical user interface (GUI). This information is derived from the **zAware** page as described in Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67. The URL includes the IP address or host name assigned to the IBM zAware partition:
`https://ip_address/zAware/` or `https://host_name/zAware/`
The “zAware” portion of the URL is case-sensitive.
- Make sure that the browser you plan to use meets the requirements and recommendations listed in Chapter 7, “Planning to use the IBM zAware GUI,” on page 55.
- Make sure that you have reviewed the planning considerations in “Planning persistent storage configuration and capacity” on page 35 and have a list of the storage devices that are intended for IBM zAware use at your installation.

Attention: The recommended practice is to configure the IBM zAware partition such that it has access to only those channel path identifiers (IDs), control units, and I/O devices that are required for network connectivity and storage. If this practice is not followed, an IBM zAware administrator might inadvertently assign storage devices that are in use by other partitions. To avoid the potential loss of critical system and application data on storage devices connected to the IBM zAware host system, make sure that you use the GUI to assign only those storage devices that are intended for IBM zAware use. Check with your storage administrator to make sure you select the appropriate storage devices to assign to the IBM zAware server.

- Make sure that you have reviewed the planning considerations in Chapter 6, “Planning for security,” on page 51.
If you plan to replace the default self-signed SSL certificate with a certificate signed by a certificate authority (CA) of your choice, you might need to process the CA reply before you can paste it into the appropriate field in the IBM zAware GUI, as instructed in step 3 on page 83.
 - The required format for replacement certificates is Base64 encoded X509 certificate blocks.
 - When you receive a reply from a certificate authority, the reply might contain a chain of certificates, starting with the signed server certificate, possibly followed by certificates from one or more intermediate CAs and, finally, the self-signed certificate of the CA. When you supply this information in the GUI, provide the entire certificate chain, starting with the signed server certificate through the self-signed certificate of the CA.
 - In some cases, the CA reply that you receive is delivered in a public-key cryptography standards (PKCS) #7 file. You must extract the certificates from the file before pasting them into the GUI. One method of extracting certificates from a PKCS #7 file is to use the **openssl pkcs7** command; for more information, see the OpenSSL Project web site at the following URL.
`http://www.openssl.org/`
- If you plan to use an existing Lightweight Directory Access Protocol (LDAP) server to authorize access to the IBM zAware GUI, the network administrator must have configured network connections to

ensure that the IBM zAware server can access the LDAP server. IBM zAware cannot save LDAP settings unless it can communicate with the LDAP server when you apply the new or changed settings.

If there is a firewall between the IBM zAware partition and the LDAP server, the IBM zAware partition must be permitted to use the port that is used by the LDAP server.

About this task

Before the IBM zAware server can receive and analyze data from monitored clients, you need to configure persistent storage, set up security, and configure settings for the analytics engine. You can accomplish most of these tasks through the IBM zAware GUI, using the default master user ID.

When you log in to the IBM zAware GUI for the first time, the browser displays a warning message because the default Secure Sockets Layer (SSL) certificate used by the IBM zAware server is not signed by a trusted certificate authority (CA). As part of the security configuration steps in this procedure, you can resolve this error by replacing the default SSL certificate with a certificate signed by a certificate authority of your choice. Doing so provides secure communication between the IBM zAware server and the browsers of all authorized users.

If you decide to replace the automatically generated certificate, which is the recommended practice for improved security, you can use any third-party certificate authority of your choice, or your installation can provide an internal certificate authority for certificate signing tasks. IBM zAware does not renew these replacement certificates; in this case, managing replacement certificates becomes the responsibility of the security administrator. The Open Directory Project maintains a list of third-party certificate authorities at the following URL.

http://www.dmoz.org/Computers/Security/Public_Key_Infrastructure/PKIX/Tools_and_Services/Third_Party_Certificate_Authorities/

Also as part of the security configuration steps in this procedure, you can authorize users to access the IBM zAware GUI through the use of an LDAP repository. You can configure user authentication through an LDAP repository or, alternatively, through the use of a local file-based repository. For simplicity, using an LDAP repository only is the preferred option. However, you might want to define one or two user IDs in a local repository so you can access the IBM zAware GUI when the LDAP server is unavailable. If you configure an LDAP repository and also define users or groups in a local repository, both sets of users or groups are available through the IBM zAware GUI.

Procedure

1. From a browser, enter the URL for the IBM zAware GUI to display the landing page.

The URL includes the IP address or host name assigned to the IBM zAware partition:

`https://ip_address/zAware/` or `https://host_name/zAware/`

Figure 29 on page 81 shows the landing page for the IBM zAware GUI.

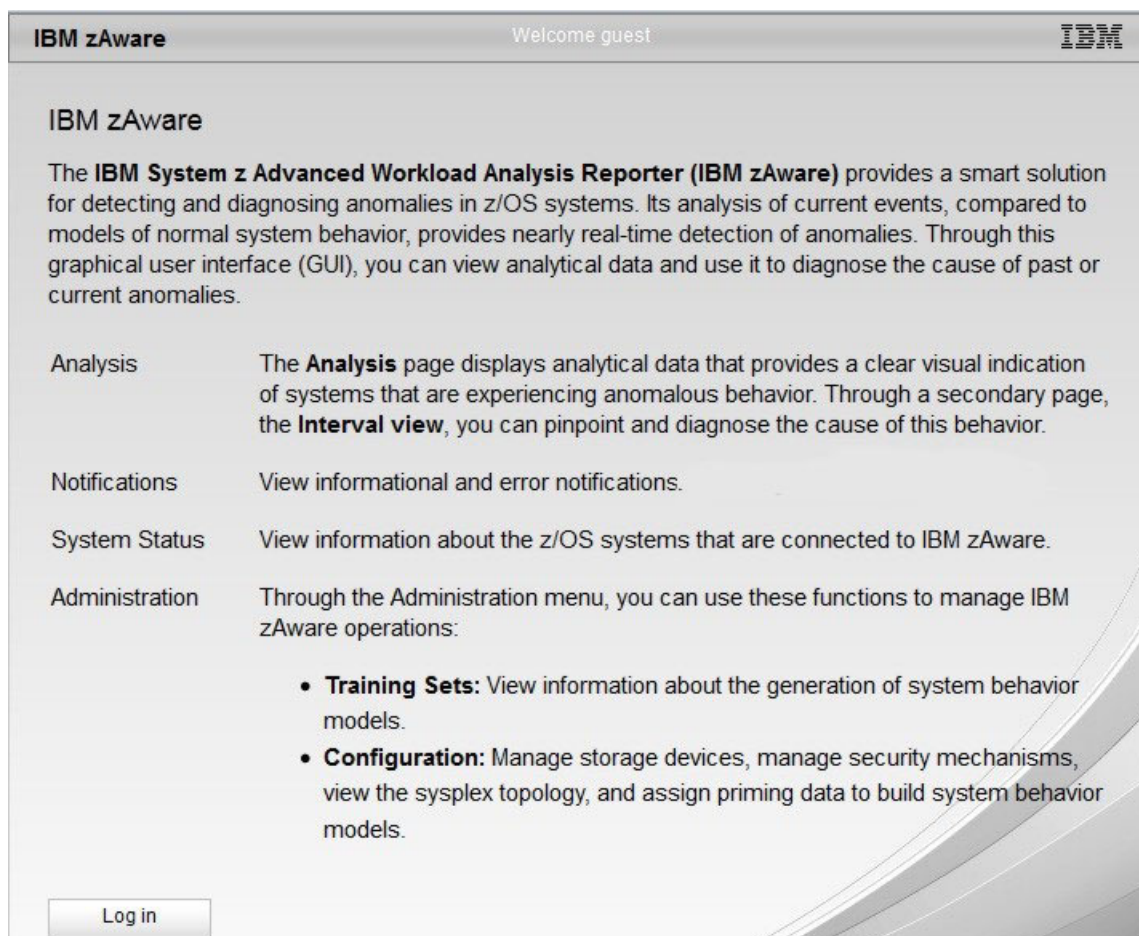


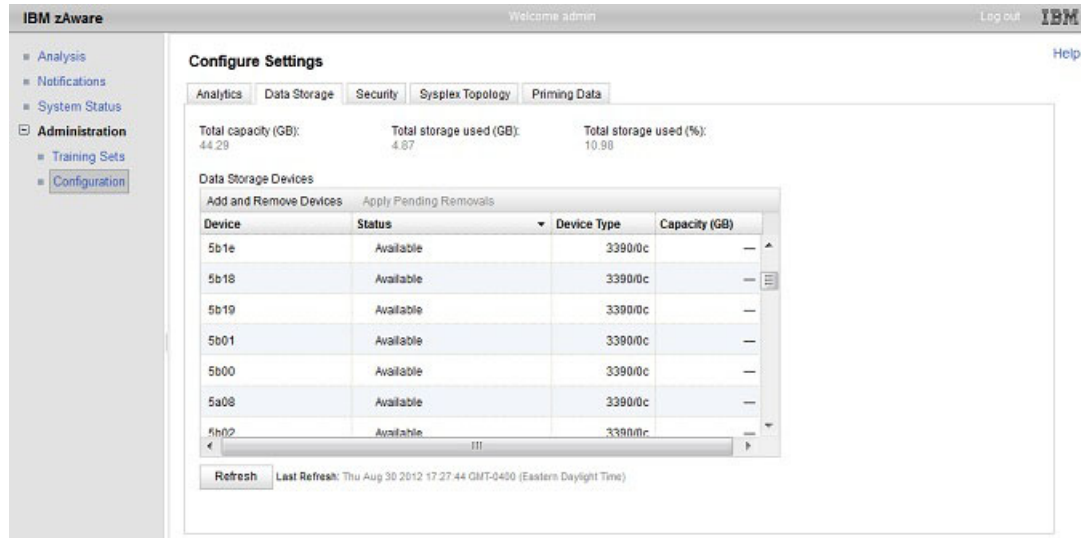
Figure 29. The landing page for IBM zAware

- If the browser presents a warning message because it does not recognize the default SSL certificate for the IBM zAware server, bypass the warning message by adding a security exception. Step 3 on page 83 explains how to replace the default SSL certificate with another certificate to permanently prevent this error.
 - Click **Log in** to display the zAware user login window.
 - Enter the default master user ID and password and click **Log in**.
 - If the **Administration** category in the navigation pane is not expanded, click the + icon to display the administration tasks. Click **Configuration** to display the **Configure Settings** page.
- Assign storage devices for the IBM zAware server to use for storing analysis results, system behavior models, and data from monitored clients.

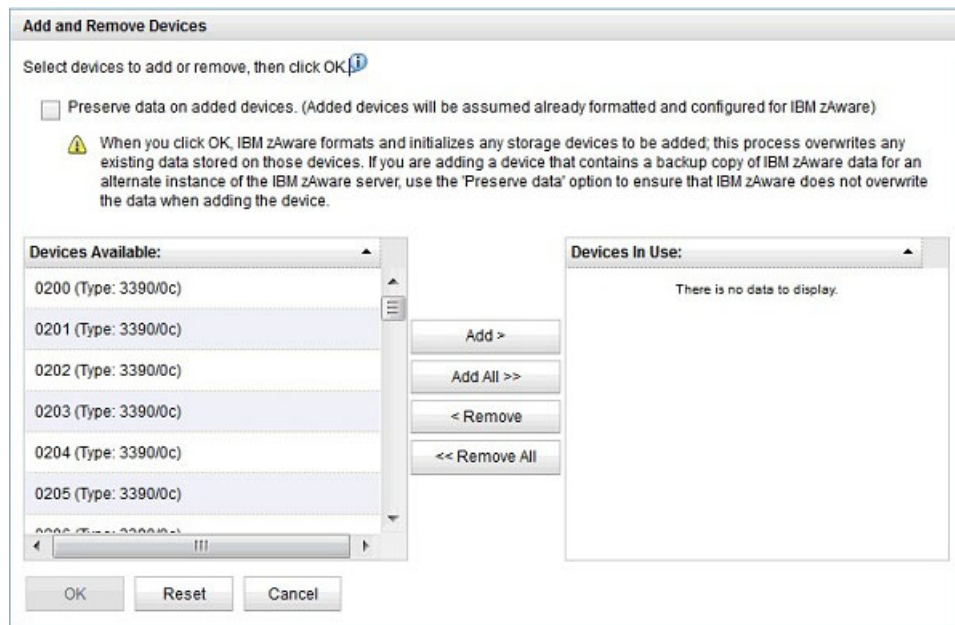
Attention: The recommended practice is to configure the IBM zAware partition such that it has access to only those channel path identifiers (IDs), control units, and I/O devices that are required for network connectivity and storage. If this practice is not followed, an IBM zAware administrator might inadvertently assign storage devices that are in use by other partitions. To avoid the potential loss of critical system and application data on storage devices connected to the IBM zAware host system, make sure that you use the GUI to assign only those storage devices that are intended for IBM zAware use. Check with your storage administrator to make sure you select the appropriate storage devices to assign to the IBM zAware server.

- Click the **Data Storage** tab on the **Configure Settings** page. The GUI populates the **Data Storage Devices** table with a list of the devices that are available and connected to the IBM zAware partition. Note that you can sort the list by clicking any one of the column headings in the **Data Storage Devices** table. Until you assign these devices to the IBM zAware server, their status is

“Available”.



- b. On the **Data Storage** page, click **Add and Remove Devices**. The GUI presents the Add and Remove Devices window.



- c. To add a storage device for the IBM zAware server to use, select one or more devices in the **Devices Available** list and click either **Add >** or **Add All >>** to move the devices to the **Devices in Use** list. You do not have to assign all devices in the list unless the server requires the total capacity.

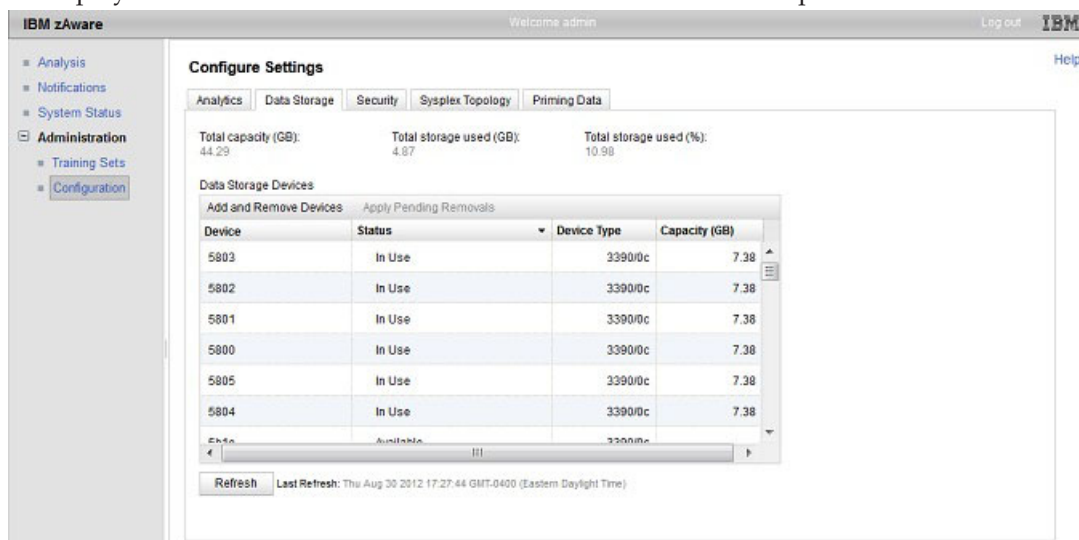
Attention: Do not use **Add All** if any of the available storage devices are shared. If a device is shared and in use by another application, data will be lost or overwritten if the IBM zAware server formats the device.

Although the IBM zAware GUI provides a **Preserve data** option for adding storage devices, which prevents IBM zAware from overwriting data on the device to be added, use this option only when assigning a storage device that contains a backup copy of IBM zAware data.

- d. When you have finished moving devices to the **Devices in Use** list, click **OK** to assign those devices.

The IBM zAware server formats the devices that you moved to the **Devices in Use** list. While the formatting process is in progress, the device status is “Being Added”; when the formatting process is complete, the device status is “In Use”. As part of the formatting process, the volume serial (VOLSER) for the device is renamed.

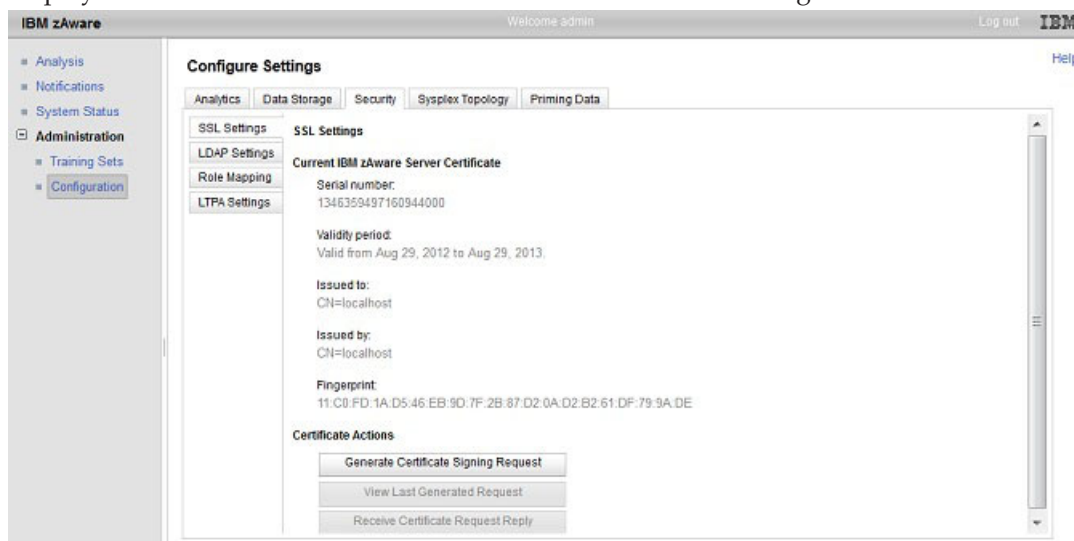
Depending on the number of devices that you assign, this formatting process might take some time. For example, IBM test experiences indicate that the IBM zAware server requires approximately 10 minutes to format and initialize a 3390 model 9 device. Periodically click **Refresh** to update the information in the **Data Storage Devices** table and sort by clicking the **Status** column heading twice, to display the devices with status other than “Available” at the top of the list.



3. Optional: Secure the communication between the IBM zAware server and browsers by generating a request for an SSL certificate and importing the reply from the certificate authority.

This process might take several days to complete, depending on the time that the certificate authority requires to receive and process your request, and to send a reply back to you. You can complete other tasks in the IBM zAware GUI while you wait for a reply from the certificate authority.

- a. Click the **Security > SSL Settings** tab on the **Configure Settings** page. The **SSL Settings** tab displays information about the default SSL certificate that is configured in the IBM zAware server.



- b. Under Certificate Actions, click **Generate Certificate Signing Request** to create a certificate signing request (CSR) to send to the certificate authority of your choice. Provide the appropriate information for the fields in Table 20 on page 84.

Table 20. Fields displayed on the page before the CSR is generated

| Field | Description |
|---------------------|---|
| Common name | Verify the host name or IP address of the IBM zAware partition. IBM zAware preloads this field with a value that matches the host name or IP address specified on the zAware page in the image profile of the IBM zAware partition. The host name is required. |
| Organization | Enter the name of your company. The value that you supply for this field must be a string of length 1-64. The organization name is optional. |
| Organizational unit | Enter the company organization or department name. The value that you supply for this field must be a string of length 1-64. The organizational unit is optional. |
| Locality | Enter the city in which your company is located. The value that you supply for this field must be a string of length 1-128. The city is optional. |
| State or province | Enter the state or province in which your company is located. The value that you supply for this field must be a string of length 1-128. The state or province is optional. |
| Postal code | Enter the postal code for your company address. The value that you supply for this field must be a string of length 1-16. The postal code is optional. |
| Country code | Enter the two-character abbreviation for the country in which your company is located. The value that you supply for this field must be a string of length 1-2. The country code is optional. |

- c. Click **Generate** to generate the certificate request.
- d. Click ► **Generated Request Input** to display and verify the generated request input.
- e. From the Generated Request text area, copy the generated certificate signing request and submit it to the certificate authority. Follow the procedures specified by the certificate authority for submitting requests.
- f. Click **Close** to return to the main **SSL Settings** page.
- g. When you receive a reply from the certificate authority, extract the certificates, if necessary, and return to the main **SSL Settings** page.

When you receive a reply from a certificate authority, the reply might contain a chain of certificates, starting with the signed server certificate, possibly followed by certificates from one or more intermediate CAs and, finally, the self-signed certificate of the CA. When you supply this information in the GUI, provide the entire certificate chain, starting with the signed server certificate through the self-signed certificate of the CA.

See Appendix B, “Sample certificate authority (CA) reply,” on page 209 for a sample CA reply that contains a certificate chain, and for an illustration of the required format for pasting the reply into the GUI.

- h. Click **Receive Certificate Request Reply**.
- i. Paste the reply into the Certificate Authority reply text area and click **Receive** to import the CA reply into the IBM zAware server.

Make sure that you do not insert any lines or spaces between the end of one certificate and the beginning of the next certificate. When you paste certificate replies in the GUI, make sure that you include all of the content, including the header -----BEGIN CERTIFICATE----- through and including -----END CERTIFICATE-----

The main **SSL Settings** page now displays information from the received CA reply.

4. Configure the LDAP repository for storing user access information. As an alternative, you can use a local file-based repository instead of an existing LDAP repository. For instructions, see Chapter 20, “Setting up a local repository to secure access to the IBM zAware GUI,” on page 185. Do **not** define the same user ID in more than one repository; results are unpredictable.

To configure user authentication through the use of an existing LDAP repository, click the **LDAP Settings** tab on the **Security** page and supply appropriate values for the following fields. The LDAP administrator for your installation can either complete this step or provide the information that you need to do so.

When you or the LDAP administrator have entered values for all required fields and any optional fields that you want to specify, click **Apply** to store these LDAP configuration values. If necessary, click **Restore** to restore the LDAP configuration values that were in effect before you clicked **Apply**.

When you click **Apply**, the GUI displays a confirmation message to indicate that the web server must be restarted for your changes to be applied. This process might take a considerable amount of time to complete. Click **OK** to confirm that you want to apply your changes, or click **Cancel**.

Table 21. General LDAP settings

| Setting | Description |
|-------------------------|---|
| LDAP server hostname | Enter the resolvable host name or IP address of the LDAP server to which you want to connect. The host name is required. |
| LDAP server port | Enter the port on which the LDAP server listens for TCP/IP connections. The value can range from 0 - 65535. The port is required. |
| Follow referrals | <p>A referral is an entity that is used to redirect a client request to another LDAP server. A referral contains the names and locations of other objects. It is sent by the server to indicate that the information the client requested can be found at another location, possibly at another server or several servers.</p> <p>Select one of the following options:</p> <p>Follow Indicates that referrals to other LDAP servers will be followed.</p> <p>Ignore Indicates that referrals to other LDAP servers will be ignored. This option is selected by default.</p> <p>A selection is required.</p> |
| Bind distinguished name | Enter the distinguished name used to bind to the LDAP repository. The name must be a string of length 0-512. If no name is specified, the server binds anonymously. The name is optional. |
| Bind password | Enter the password used to bind to the LDAP directory. The password must be a string of length 0-512. The password is optional. |
| Base distinguished name | Enter the distinguished name of a base entry in the repository. The name must be a string of length 1-512. The name is required. |
| Login attribute | <p>Enter the LDAP attribute of a user entity used to login to the IBM zAware GUI. The attribute must uniquely identify a user in the directory.</p> <p>Typical login attributes include <i>uid</i>, <i>mail</i>, <i>primaryuserid</i>, and so on. The value must be a string of length 1-512. The default value is <i>uid</i>. The login attribute is required.</p> |
| User object classes | <p>Enter the object class or classes that are associated with user entities in the LDAP repository. Delimit multiple object classes with semicolons (;).</p> <p>Typical object classes include <i>Person</i>, <i>ePerson</i>, <i>inetOrgPerson</i>, and so on. The value must be a string of length 1-512. At least one user object class is required.</p> |
| User search bases | <p>Specify the base object of the directory (or level of the directory) from which to start a search for user entities in the LDAP repository. The search bases must be subtrees of the base distinguished name. Delimit multiple search bases with semicolons (;).</p> <p>The value must be a string of length 1-512. The user search base is optional. If unspecified, the base distinguished name is used.</p> |
| SSL enabled | Select this option to enable secure socket communication to the LDAP server. If selected, you must supply the SSL certificate in the LDAP server certificate field. By default, SSL is disabled. |

Table 21. General LDAP settings (continued)

| Setting | Description |
|-------------------------|--|
| LDAP server certificate | Enter the Base64 encoded certificate that is required to validate the certificate of the LDAP server. This certificate should be the signer of the server certificate for the LDAP repository. A certificate is required only when SSL is enabled. |

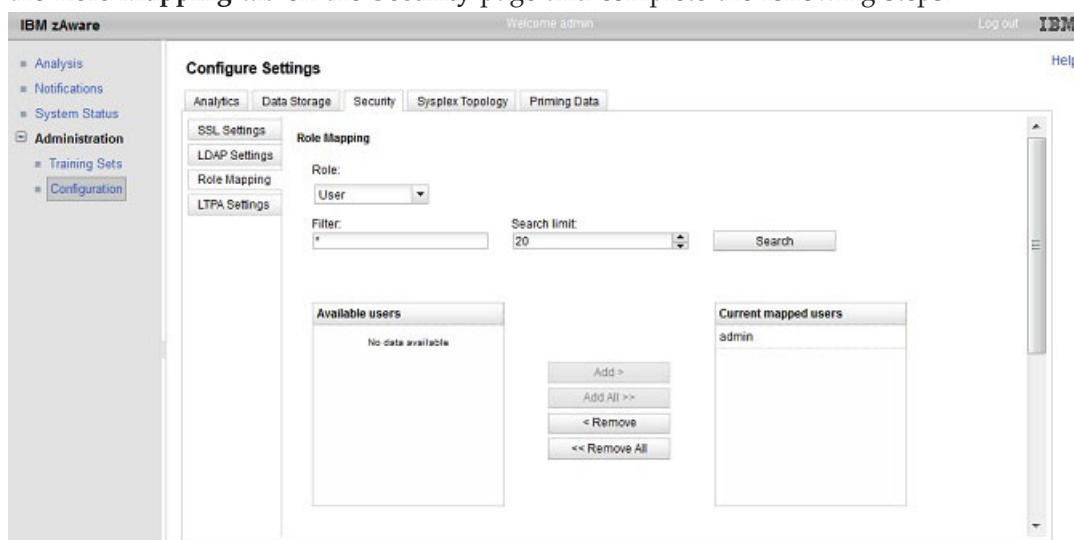
Table 22. Group LDAP settings

| Setting | Description |
|---------------------------------|---|
| User group membership attribute | Enter the LDAP attribute of a user entity that indicates the groups to which an entry belongs. If your LDAP server does not support the group membership attribute, do not specify this attribute. The value must be a string of length 1-512. The user group membership attribute is optional. |
| User group membership scope | <p>Select the scope of the user group membership attribute. You can select one of the following options:</p> <p>Direct Indicates that the attribute contains only immediate members of the group without members of subgroups. This option is selected by default.</p> <p>Nested Indicates that the attribute contains direct members and members nested within subgroups of this group.</p> <p>All Indicates that the attribute contains all direct, nested, and dynamic members.</p> <p>A selection is required if a value is specified in the User group membership attribute field.</p> |
| Group object classes | <p>Enter the object class or classes that are associated with group entities in the LDAP repository. Delimit multiple object classes with semicolons (;).</p> <p>Typical object classes include <i>groupOfNames</i>, <i>groupOfUniqueNames</i>, and so on. The value must be a string of length 1-512. At least one group object class is required.</p> |
| Group search bases | <p>Specify the base object of the directory (or level of the directory) from which to start a search for group entities in the LDAP repository. The search bases must be subtrees of the base distinguished name. Delimit multiple search bases with semicolons (;).</p> <p>The value must be a string of length 1-512. The group search base is optional. If unspecified, the base distinguished name is used.</p> |
| Group member attributes | <p>For each group object class specified in the Group object classes field, indicate the LDAP attribute of a group entity in the object class that contains the members of the group. Delimit multiple group member attributes with semicolons (;). A value is required, and must be a string of length 1-512.</p> <p>For example, if the group object classes specification is <i>groupOfNames;groupOfUniqueNames</i>, the group member attributes specification might be <i>member;uniqueMember</i>.</p> |
| Group member object classes | For each attribute specified in the Group member attributes field, specify the object classes of the group that uses the member attribute. The value must be a string of length 1-512. The group member object classes are optional. If unspecified, the member attributes apply to all group object classes. |

Table 22. Group LDAP settings (continued)

| Setting | Description |
|--------------------|--|
| Group member scope | <p>Select the scope of the group member attribute. You can select one of the following options:</p> <p>Direct Indicates that the member attribute contains only direct members. This option is selected by default.</p> <p>Nested Indicates that the member attribute contains both direct and nested members.</p> <p>All Indicates that the member attribute contains direct, nested, and dynamic members.</p> <p>A selection is required.</p> |

5. Authorize users or groups to access the IBM zAware GUI. You can map authorized users and groups to specific roles: either **Administrator** or **User**. Users or groups with Administrator authority can use any task in the GUI, while those with User authority can view only the following pages and use only the actions as noted:
 - On the graphic or tabular **Analysis** page, all controls and actions are permitted.
 - On the **Interval view**, all controls and actions are permitted except for modifying the non-IBM rules status for a specific message ID. Only administrators can view and change a rules status value. IBM rules cannot be changed.
 - On the **Notifications** page, all actions are disabled.
 - On the **System Status** page, all actions are disabled.
- a. Through the IBM zAware GUI, map users or groups in the LDAP repository to specific roles. Click the **Role Mapping** tab on the **Security** page and complete the following steps.



- 1) Select either **Administrator** or **User** as the role to which you want to map particular users or groups. The IBM zAware server populates the **Current mapped users** and **Current mapped groups** lists with all users or groups that are currently mapped to the selected role. Initially, only the default master user ID appears in the **Current mapped users** list for both the Administrator role and the User role.
- 2) To add users or groups to the selected role, provide a filter value to populate the **Available users** and **Available groups** lists with matching user and group entries in the LDAP repository. You can specify an asterisk (*) as a wildcard value at any position in the filter value. An asterisk (*) is the default filter value.
- 3) Enter a search limit value to limit the number of matching entries that display in the **Available groups and users** list. This limit applies to both groups and users so a search limit of 20 might

return 40 entries: 20 groups and 20 users. The default value for this limit is 20. You can replace the default value with any value from 1 through 200.

- 4) Click **Search** to apply the filter and search limit values. The IBM zAware server populates the **Available users** and **Available groups** lists with entries that match the filter value, up to the search limit value.
- 5) To add a user or group to the selected role, select one or more entries in the **Available users** and **Available groups** lists and click either **Add >** or **Add All >>** to copy the entries to the **Current mapped users** and **Current mapped groups** lists.
- 6) When you have finished adding entries to the **Current mapped users** and **Current mapped groups** lists, click **Apply** to store your changes in the LDAP repository. You might need to scroll down the page to find **Apply**.
- 7) The IBM zAware GUI displays the Apply Role Mappings window, through which you can check the role assignments that you have selected. If the changes are correct, click **Apply**; if you need to make further changes, click **Cancel** to return to the **Role Mapping** tab.

When you click **Apply**, the GUI displays a confirmation message to indicate that the web server must be restarted for your changes to be applied. This process might take a considerable amount of time to complete. Click **OK** to confirm that you want to apply your changes, or click **Cancel**.

6. Optional: Change the configuration value that determines the duration of a browser session.

By default, browser sessions time out after 12 hours (720 minutes). To change this setting, complete the following steps.

- a. Click the **LTPA Settings** tab on the **Security** page.
- b. In the **LTPA timeout** field, click the arrows to select a value in minutes. The allowable range of values is 10-525600 minutes (365 days).
- c. Click **Apply** to save the new value.

When you click **Apply**, the GUI displays a confirmation message to indicate that the web server must be restarted for your changes to be applied. This process might take a considerable amount of time to complete. Click **OK** to confirm that you want to apply your changes, or click **Cancel**.

7. If necessary, update firewall settings to ensure secure communications between the IBM zAware server and its monitored clients.

Although the recommended configurations in Chapter 4, “Planning your IBM zAware environment,” on page 19 show both the IBM zAware server and its monitored clients within the boundary of a firewall, you can set up a configuration in which communication crosses firewall boundaries. In this case, you need to determine whether unsecured communication is an acceptable risk. If it is not an acceptable risk, you must provide your own method of securing this communication. For additional information, see “Securing communication between IBM zAware and its monitored clients” on page 51.

8. Optional: Check the configuration values that control IBM zAware analytics operation and adjust them, if necessary. Click the **Analytics** tab on the **Configure Settings** page.

All fields on the **Analytics** page contain default values that represent reasonable estimates for IBM zAware analytics. These estimates might not be appropriate for monitored clients at your installation, so you might need to change the default values according to your knowledge of client workloads.

If you increase the retention times of instrumentation data, training models, or analysis results, you might need to increase the amount of persistent storage that the IBM zAware can use. To determine whether you need to add storage devices, periodically use the **Data Storage** page to monitor the list of assigned storage devices, their current status, and capacity.

The values on this page are global settings that apply for all monitored clients. You cannot specify different date ranges for individual monitored clients but you can manage the training dates used for each monitored client through the **Administration > Training Sets** page.

If you alter any of the default values on the **Analytics** page, click **Apply** to save them.

IBM zAware

Welcome admin

Log out IBM

Help

■ Analysis
■ Notifications
■ System Status
■ Administration
■ Training Sets
■ Configuration

Configure Settings

Analytics Data Storage Security Sysplex Topology Priming Data

Instrumentation data retention time (training period - 730 days):
365 days

Training models retention time (0 - 730 days):
365 days

Analysis results retention time (30 - 3650 days):
365 days

Training period (1 - 365 days):
90 days

Training Interval (7 - 365 days):
7 days

Apply Reset

Instrumentation data retention time

Specifies the number of consecutive calendar days for which the IBM zAware server keeps the data received from monitored clients. This data provides the source for training models so the retention time must match or exceed the duration specified for **Training period**.

For example, if you specify 90 days:

- The server stores client data for 90 consecutive days, whether or not instrumentation data is available on each of the days between that date range.
- Periodically, the server deletes data that is older than 90 days.

IBM zAware uses this value to periodically remove outdated information through an automated process that runs daily.

Default value: 365 days

Valid range: 1 through 730

Training models retention time

Specifies the number of consecutive calendar days for which the IBM zAware server keeps training models for all monitored clients. If you enter 0 as the retention time, the server keeps only the current training model for each monitored client.

IBM zAware uses this value to periodically remove outdated information through an automated process that runs daily.

Default value: 365 days

Valid range: 0 through 730

Analysis results retention time

Specifies the number of consecutive calendar days for which the IBM zAware server keeps analysis results for all monitored clients.

IBM zAware uses this value to periodically remove outdated information through an automated process that runs daily.

Default value: 365 days

Valid range: 30 through 3650

Training period

Specifies the number of consecutive calendar days that the IBM zAware server uses to identify the instrumentation data to include in training models. The instrumentation data received on days during this time period serves as input for creating the model of normal system

behavior for each monitored client. If the monitored clients at your installation process workloads in a six-month cycle, for example, you can change the value to 180 days.

The server builds a training model from the instrumentation data received during this time period, whether or not data is available for each day.

Default value: 90 days

Valid range: 1 through 365

Training interval

Specifies the number of consecutive calendar days between automatic builds of system behavior models.

| IBM zAware uses this value to schedule automated builds only after the initial client model is
| built successfully. For an automated build to be scheduled, the client must be connected to the
| IBM zAware server.

Default value: 30 days

Valid range: 7 through 365

After you click **Apply** to store new configuration values for analytics operation, the IBM zAware GUI displays a message that indicates whether it successfully stored your changes.

Results

The IBM zAware server is fully configured and ready to receive data from monitored clients.

What to do next

Follow the procedure in Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91.

Chapter 12. Configuring z/OS monitored clients to send data to the IBM zAware server

Use this procedure as an overview for configuring z/OS monitored clients to send data to the IBM zAware server for analysis. This procedure is intended primarily for skilled z/OS system programmers who have experience with configuring and managing systems in a Parallel Sysplex. Depending on the roles and responsibilities defined for your IT organization, you might need the assistance of network or security administrators to correctly configure secure connectivity within the IBM zAware environment.

Before you begin

- Make sure that your installation has completed the following steps for defining network connections for the hardware in the IBM zAware environment:
 - Step 1 on page 64 in Chapter 9, “Configuring network connections and storage for the IBM zAware partition,” on page 63.
 - Step 7 on page 75 in Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67.

Consider using the checklist in “Task summary and configuration checklist for network administrators” on page 34 as an aid for step 1 on page 92 in this procedure.

- Make sure that your installation has completed the procedure in Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79.
- List the z/OS systems to become monitored clients of the IBM zAware server. For information about the types of z/OS systems to monitor, see Chapter 4, “Planning your IBM zAware environment,” on page 19.

IBM zAware supports z/OS systems that run in z/OS partitions or as z/VM guests. The number of clients is limited only by the resources assigned to the IBM zAware partition. z/OS monitored clients must meet the following requirements:

- The system must be configured as a single-system sysplex (monoplex), a system in a multisystem sysplex, or a member of a Parallel Sysplex.
- The system must be running one of the following releases of the z/OS operating system.
 - z/OS Version 2 Release 1 (V2R1) or a later release. APAR **OA42095** is required for z/OS V2R1 only if the z/OS bulk load client is to process priming data that contains machine control characters.
 - z/OS Version 1 Release 13 (V1R13) with the following PTFs.

Table 23. Required V1R13 PTFs for z/OS monitored clients

| Component | APAR | PTF |
|--|---|--|
| BCP system logger | APAR OA38747 | PTF UA66494 HBB7780 PTF UA66495 JBB778J |
| BCP system logger | APAR OA38613 Prerequisite for APAR OA38747 | PTF UA66195 HBB7780 PTF UA66196 JBB778J |
| BCP z/OS bulk load client for IBM zAware | APAR OA39256 APAR OA42095 ¹ | PTF UA66522 HBB7780 PTF UA69292 HBB7780 PTF UA69293 HBB7780 |
| Footnote: 1. APAR OA42095 is required for z/OS V1R13 only if the z/OS bulk load client is to process priming data that contains machine control characters. | | |

- The system must be using the operations log (OPERLOG) as the hardcopy medium.
- The system name and sysplex name must uniquely identify the system to be monitored. IBM zAware identifies each monitored client by sysplex and system name, in the format *sysplex_name.system_name*; for example: SYSPLEX1.SYSA. IBM zAware cannot monitor more than one system with the same sysplex and system name combination.
- Log in to the z/OS system with a user ID that has the authority to complete the following tasks.
 - Access and modify members of the SYS1.PARMLIB data set.
 - Access and modify the LOGR couple data set and log stream usage.
 - Access the z/OS USS segment.

To determine the authority required to issue specific z/OS commands to accomplish these tasks, see the list of MVS™ commands, z/OS Security Server (RACF®) access authorities and resource names in *z/OS MVS System Commands*, SA22-7627.

About this task

This procedure provides an overview of the steps required to configure each z/OS monitored client to send operations log (OPERLOG) data to the IBM zAware server. The details for each step are documented in various books in the z/OS product library; in this procedure, the appropriate books are listed for your reference. The z/OS product library is available in the z/OS Internet Library web site at <http://www.ibm.com/systems/z/os/zos/bkserv/>.

Table 57 on page 206 contains a summary of related updates in the z/OS product library.

Procedure

1. Configure a network connection from each z/OS monitored client to the IBM zAware server. To determine whether this network configuration step is required, you can ping the IBM zAware server from z/OS system. From the TSO command panel or the READY prompt on the z/OS system, enter the **PING** or **TRACERTE** command with either the IP address or host name of the IBM zAware server. If the command is successful, skip to step 2 on page 93.
 - a. Update the TCP/IP profile for the z/OS monitored client, as necessary, for the channel paths that are assigned to the IBM zAware server.
 - For Ethernet connectivity, use an **INTERFACE** statement to define an **IPAQENET** or **IPAQENET6** interface with **CHPIDTYPE OSD**.
 - For connectivity through the intraensemble data network (IEDN), use an **INTERFACE** statement to define an **IPAQENET** or **IPAQENET6** interface with **CHPIDTYPE OSX**. Specify the **CHPID** parameter with the 2-character hexadecimal value that matches the value specified on the **CHPID** type **OSX** definition statement for the IBM zAware host system.
 - For connectivity through HiperSockets, use a **DEVICE** and **LINK MPCIPA** statement to define the HiperSockets device. Specify a device name of **IUTIQDxx**, where **xx** is the **CHPID** number that matches the hexadecimal value specified on the **CHPID** type **IQD** definition statement for the IBM zAware host system.

Make sure that the z/OS client is configured to use layer 3 to connect to the IBM zAware server. If you make any changes to the domain name system (DNS) or local host file, you need to refresh the resolver.

- b. Start the modified TCP/IP stacks. For example, use the **VARY TCPIP** command to start the desired device, where *tcpiproc* is the name of the TCP/IP profile and *devicename* is the name of the device:


```
VARY TCPIP,tcpiproc,START,devicename
```
 - c. Verify the TCP/IP connection between the z/OS monitored client and the IBM zAware server. To verify the status of devices and links defined to the TCP/IP stack, use the **DISPLAY TCPIP** command to request **NETSTAT** information. For example:


```
D TCPIP,procname,NETSTAT,DEVLINKS
```


In the resulting display, check for the following:

- The device name and type match the TCP/IP profile definitions and the device is in a ready status.
 - The link name and type match the TCP/IP profile definitions and the link is in a ready status.
- d. If necessary, update firewall settings to ensure secure communications between the IBM zAware server and its monitored clients.

Although the recommended configurations in Chapter 4, “Planning your IBM zAware environment,” on page 19 show both the IBM zAware server and its monitored clients within the boundary of a firewall, you can set up a configuration in which communication crosses firewall boundaries. In this case, you need to determine whether unsecured communication is an acceptable risk. If it is not an acceptable risk, you must provide your own method of securing this communication. For additional information, see “Securing communication between IBM zAware and its monitored clients” on page 51.

For additional details, see the following books:

- *z/OS Communications Server: IP Configuration Guide*
- *z/OS Communications Server: IP Configuration Reference*
- *z/OS Communications Server: IP System Administrator's Commands*

2. Configure the z/OS monitored client as a single-system sysplex (monoplex), a system in a multisystem sysplex, or a member of a Parallel Sysplex. To determine whether the z/OS monitored client is configured correctly already, issue the **DISPLAY XCF,SYSPLEX,ALL** command and check the resulting message display for the system mode.

If message IXC337I indicates that the system is running in XCF-LOCAL mode, modify the PLEXCFG parameter in the IEASYSxx parmlib member for the z/OS client. Specify one of the following parameter values:

- PLEXCFG=MONOPLEX for a single-system sysplex
- PLEXCFG=MULTISYSTEM for a system in a multisystem sysplex or a member of a Parallel Sysplex

You can specify PLEXCFG=ANY, in which case the system mode is determined by settings in the COUPLExx and CLOCKxx parmlib members. In this case, make sure that those parmlib settings *do not* result in the z/OS monitored client running in XCF-LOCAL mode.

For additional details, see the following topics:

- “Planning parmlib members for a sysplex” in *z/OS MVS Setting Up a Sysplex*, SA22-7625.
- IEASYSxx, COUPLExx, and CLOCKxx parmlib member descriptions in *z/OS MVS Initialization and Tuning Reference*, SA22-7592.

3. Configure the z/OS system logger to send data to the IBM zAware server. The following steps provide an overview of the required updates for the system logger. The primary references for details are:

- Planning topics in *z/OS MVS Setting Up a Sysplex*, including “Preparing for z/OS IBM zAware log stream client usage.”
- Parmlib member descriptions in *z/OS MVS Initialization and Tuning Reference*.

- a. Make sure the LOGR CDS format level is at least HBB7705.

To determine what format level is in use for a sysplex, enter the following command and check the resulting message display.

```
D XCF,COUPLE,TYPE=LOGR
```

If the LOGR CDS format level is not HBB7705, your installation needs to run the format CDS utility IXCL1DSU with the DATA TYPE(LOGR) and ITEM NAME(SMDUPLEX) NUMBER(1) options. For additional information, see the topic on LOGR parameters for the format utility in *z/OS MVS Setting Up a Sysplex*.

- b. Set up the authority that the z/OS system logger requires to send data to the IBM zAware server.
- For TCP/IP connectivity to the IBM zAware server, the IXGLOGR address space must have security permission for a z/OS UNIX System Service segment.

- To define or update a log stream that contains data to be sent to the IBM zAware server, the user must have Security Authorization Facility (SAF) update access to the IXGZAWARE_CLIENT resource in the FACILITY class.

c. Configure SYS1.PARMLIB members that define or control system logger operations.

- 1) Create an IXGCNFxx parmlib member to define communication and log buffering details. Specify the ZAI statement with the following parameters:

SERVER(*host_name*|*IP_address*)

Specifies the host name (as defined by the DNS server) or the IPv4 or IPv6 address that identifies where the IBM zAware server is running. If the z/OS client is connecting to the IBM zAware server over a network that uses the Dynamic Host Connection Protocol (DHCP), you must specify the host name for the IBM zAware partition.

PORT(*number*)

Identifies the port number associated with the IBM zAware server. The port number is 2001.

LOGBUFMAX(*value*)

Identifies the maximum amount of storage buffers (in gigabytes) to be used by system logger for managing z/OS monitored client data that is being sent to the IBM zAware server.

LOGBUFWARN(*nn*)

Identifies the amount (as a percentage) of used buffer space for which the z/OS system logger starts issuing the error message IXG375E.

LOGBUFFULL(*MSG*|*QUIESCE*)

Specifies the action that the z/OS system logger is to take when the log stream buffers become full.

The following example shows the **ZAI** statement with parameters and sample values:

```
ZAI
  SERVER(zserver.loc.com)
  PORT(2001)
  LOGBUFMAX(1)
  LOGBUFWARN(80)
  LOGBUFFULL(MSG)
```

- 2) Add the IXGCNFxx system parameter to the IEASYSxx parmlib member. This system parameter specifies the IXGCNFxx parmlib member to be used when the z/OS system logger starts or is restarted. In the IEASYSxx parmlib member, use the syntax format IXGCNF=xx

d. Issue the **SET IXGCNF=xx** command to apply the updated system logger configuration.

4. Use the **DISPLAY LOGGER** command to verify the configuration updates. The following **DISPLAY** command requests the z/OS system logger to use current configuration options to communicate with the IBM zAware server.

```
DISPLAY LOGGER,STATUS,ZAI,VERIFY
```

The resulting display contains general system logger status, the state of the z/OS monitored client, and ZAI statement parameter options, along with an indication of whether the “verify communication” request succeeded or failed. If the display contains “ZAI VERIFY INITIATED”, check for messages in the range IXG37x-IXG38x with the text “DISPLAY ZAI,VERIFY” included for the verification results. The following system logger message indicates successful communications between the z/OS monitored client and the IBM zAware server:

```
IXG380I ZAI LOGSTREAM CLIENT ESTABLISHED FOR DISPLAY ZAI,VERIFY
```

For additional information about the **DISPLAY LOGGER** command, see *z/OS MVS System Commands*.

5. Determine whether the z/OS monitored client is using OPERLOG as the hardcopy medium. Issue the **DISPLAY CONSOLES** command and check the resulting message display for information about the hardcopy medium.

- If message CNZ4100I indicates that the system is not configured to use OPERLOG, continue to step 6.
 - If message CNZ4100I indicates that the system is using OPERLOG already, complete the following steps.
- a. Update the existing OPERLOG log stream with the parameters required for IBM zAware.

ZAI(YES)

Specifies that the log stream data is to be sent to the IBM zAware server.

ZAIDATA('value')

Provides an optional value to be passed to the IBM zAware server. For example, you can specify 'OPERLOG' as the value for the ZAIDATA keyword.

To update the OPERLOG log stream with the administrative data utility IXCMIAPU, use a SYSIN DD statement similar to the following sample.

```
//SYSIN DD *
DATA TYPE(LOGR) REPORT(YES)
UPDATE LOGSTREAM NAME(SYSPLEX.OPERLOG)
ZAI(YES)
ZAIDATA('OPERLOG')
```

- b. Create the required security definitions for the z/OS Security Server (RACF), or an equivalent security product, to allow users to browse the operations log. In the following example, the SYSPLEX.OPERLOG of the LOGSTRM resource CLASS is given READ permission, which allows all users to browse the operations log. *userid1* has UPDATE access level, which allows *userid1* to delete records from the log stream.

```
RDEFINE LOGSTRM SYSPLEX.OPERLOG UACC(READ)
PERMIT SYSPLEX.OPERLOG CLASS(LOGSTRM) ID(userid1)
ACCESS(UPDATE) SETROPTS CLASSACT(LOGSTRM)
```

- c. Continue to step 7 on page 96.

6. Configure the z/OS monitored client to use OPERLOG as the hardcopy medium. Use the following steps as a model for configuring OPERLOG at your installation.

- a. Using the administrative data utility IXCMIAPU, define the corresponding coupling facility structure in the coupling facility resource management (CFRM) policy. For example:

```
STRUCTURE NAME(OPERLOG)
SIZE(40448)
INITSIZE(40448)
PREFLIST(FACIL01,FACIL02)
```

- b. Activate the CFRM policy. You can activate the policy through the COUPLExx parmlib member or through the SETXCF command. For example:

```
SETXCF START,POLICY,TYPE=CFRM,POLNAME=policy_name
```

- c. Create the OPERLOG log stream, using the following parameters that are required for IBM zAware.

ZAI(YES)

Specifies that the log stream data is to be sent to the IBM zAware server.

ZAIDATA('value')

Provides an optional value to be passed to the IBM zAware server. For example, you can specify 'OPERLOG' as the value for the ZAIDATA keyword.

The following sample illustrates JCL and control statements for using the administrative data utility to define an OPERLOG log stream:

```
//OPERLOG JOB CLASS=A,MSGCLASS=A
//POLICY EXEC PGM=IXCMIAPU
//SYSPRINT DD SYSOUT=A
//SYSIN DD *
DATA TYPE(LOGR)
```

```

DEFINE STRUCTURE NAME(OPERLOG)
LOGSNUM(1)
MAXBUFSIZE(4092)
AVGBUFSIZE(512)
DEFINE LOGSTREAM NAME(SYSplex.OPERLOG)
STRUCTNAME(OPERLOG)
LS_DATACLAS(LOGR24K)
HLQ(IXGLOGR)
LS_SIZE(2560)
LOWOFFLOAD(0)
HIGHOFFLOAD(80)
STG_DUPLEX(NO)
RETPD(0)
AUTODELETE(NO)
ZAI(YES)
ZAIDATA('OPERLOG')

```

- d. Create the required security definitions for the z/OS Security Server (RACF), or an equivalent security product, to allow users to browse the operations log. In the following example, the SYSplex.OPERLOG of the LOGSTRM resource CLASS is given READ permission, which allows all users to browse the operations log. *userid1* has UPDATE access level, which allows *userid1* to delete records from the log stream.

```

RDEFINE LOGSTRM SYSplex.OPERLOG UACC(READ)
PERMIT SYSplex.OPERLOG CLASS(LOGSTRM) ID(userid1)
ACCESS(UPDATE) SETROPTS CLASSACT(LOGSTRM)

```

- e. Define the hardcopy device as OPERLOG in the HARDCOPY statement of the CONSOLxx parmlib member. You can change this setting using the **VARY** command:

```
V OPERLOG,HARDCPY
```

- f. If your system is configured as a monoplex, create a DASD-only log stream for OPERLOG. To create a DASD-only log stream, you need to define or update the system logger couple data set (LOGR CDS) with a large enough log stream records (LSR) value to allow sufficient space for managing the DASD-only log stream for this z/OS monitored client. Review the planning considerations in *z/OS MVS Setting Up a Sysplex*, including the topics about planning DASD space for system logger and managing log data.

For more information about setting up OPERLOG, see the topic on preparing to use system logger applications in *z/OS MVS Setting Up a Sysplex*.

7. Start sending log stream data to the IBM zAware server. Issue the **SETLOGR** command:

```
SETLOGR FORCE,ZAICONNECT,LSNAME=SYSplex.OPERLOG
```

The **ZAICONNECT** parameter directs system logger to attempt a socket connection from the z/OS monitored client to the IBM zAware server, as defined in the current IXGCNFxx parmlib member.

The system responds with the following messages:

```

IXG651I SETLOGR FORCE ZAICONNECT COMMAND ACCEPTED FOR LOGSTREAM=SYSplex.OPERLOG
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR LOGSTREAM SYSplex.OPERLOG
STATUS: ATTEMPTING SOCKET CREATE
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR LOGSTREAM SYSplex.OPERLOG
STATUS: SOCKET CREATE SUCCESSFUL
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR LOGSTREAM SYSplex.OPERLOG
STATUS: ATTEMPTING SOCKET CONNECT
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR LOGSTREAM SYSplex.OPERLOG
STATUS: SOCKET CONNECT SUCCESSFUL
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR LOGSTREAM SYSplex.OPERLOG
STATUS: INITIATING SOCKET VALIDATION
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR LOGSTREAM SYSplex.OPERLOG
STATUS: SOCKET VALIDATION SUCCESSFUL
IXG380I ZAI LOGSTREAM CLIENT ESTABLISHED FOR LOGSTREAM SYSplex.OPERLOG

```

For detailed information about log stream status, you can issue the following **DISPLAY LOGGER** command:

```
D LOGGER,C,LSN=SYSplex.OPERLOG,D
```

The system responds with message IXG601I, as shown in the following sample:

```
IXG601I 15.40.21  LOGGERS DISPLAY FRAME 1 F E SYS=SY2
CONNECTION INFORMATION BY LOGSTREAM FOR SYSTEM SY2
LOGSTREAM          STRUCTURE          #CONN STATUS
-----
SYSplex.OPERLOG    IXGLOGR_STR1      000001 OFFLOAD IN PROGRESS
  DUPLEXING: STAGING DATA SET
  STGDSN: LOGGERS.SYSplex.OPERLOG.SY2
          VOLUME=SMSVL4 SIZE=000060 (IN 4K) % IN-USE=050
GROUP: PRODUCTION  ZAI CLIENT: YES - CONNECTED
ZAI DATA: NO_ZAI DATA
  LOG BLOCKS SENT TO SERVER OK: 00000000008, FAILED: 00000000000
JOBNAME: CONSOLE   ASID: 0009
R/W CONN: 000000 / 000001
RES MGR./CONNECTED: *NONE* / NO
LOGSTREAM          STRUCTURE          #CONN STATUS
  IMPORT CONNECT: NO

NUMBER OF LOGSTREAMS: 000001
```

For additional information about the **SETLOGR** and **DISPLAY LOGGERS** commands, see *z/OS MVS System Commands*.

Results

The z/OS system is established as an IBM zAware monitored client.

When z/OS monitored clients send current data to the IBM zAware server, the server uses both the sysplex name and system name passed in this data to uniquely identify data for a specific monitored client. To view the status for monitored clients that are sending current data, navigate to the **System Status** page in the IBM zAware GUI.

System Status

System Status displays the IBM zAware analytics engine status, as well as monitored systems information for z/OS systems connected to IBM zAware. Click the start button () to start the analytics engine, and the stop button () to stop it.

Analytics engine status: Running

IBM zAware Monitored System Data Suppliers:

| System | Sysplex | Status | Instrumentation Data Type | Connect Start Time |
|--------|----------|----------|---------------------------|--|
| SY1 | PLEX1 | Inactive | OPERLOG | August 30, 2012 4:09:04 PM Eastern Daylight Time |
| SY2 | PLEX1 | Inactive | OPERLOG | August 30, 2012 5:13:19 PM Eastern Daylight Time |
| CB8E | UTCPLXCB | Inactive | OPERLOG | August 30, 2012 2:40:37 PM Eastern Daylight Time |

[Refresh](#) Last refresh: Thu Aug 30 2012 17:19:38 GMT-0400 (Eastern Daylight Time)

What to do next

- To prime the IBM zAware server to begin data analysis as quickly as possible, follow the instructions in Chapter 13, “Creating an IBM zAware model for new z/OS monitored clients,” on page 99.
- Issue the **SETLOGR** command as necessary during normal operations for the monitored client.
 - If an unscheduled IPL or system logger restart occurs after the z/OS system is established as a monitored client, you do not have to issue the **SETLOGR** command to reconnect the client and IBM

zAware server. Following an IPL or system logger restart, communication is attempted automatically after the OPERLOG log stream is connected on the z/OS system.

- | – To prepare for a scheduled IPL, consider disconnecting the monitored client to avoid reconnection attempts and the messages associated with those attempts. For example, you can complete the following shutdown procedure:
 - | 1. Issue SETLOGR FORCE,ZAIQUIESCE with additional parameters, as necessary, to disconnect a specific or all IBM zAware log stream clients that are running on the z/OS system.
 - | 2. Follow the procedure that your installation uses to shut down TCP/IP and z/OS UNIX System Services.
- If necessary, see *z/OS Diagnosis: Reference* for information about resolving system logger errors related to log stream processing for z/OS monitored clients.

Chapter 13. Creating an IBM zAware model for new z/OS monitored clients

Use this procedure to prime the IBM zAware server with data to create a model of normal system behavior for z/OS monitored clients. The estimated amount of data for building the most accurate models is 90 days of data for each client. Your installation can modify this data requirement, which is known as the *training period* for IBM zAware analytics, based on your knowledge of the workloads running on z/OS monitored clients. Instead of waiting for the IBM zAware server to collect data over the course of the training period, however, you can prime the server by transferring prior data for monitored clients, and request the server to build a model for each client from the transferred data. This procedure provides instructions for priming the IBM zAware server and building a model from the priming data. This procedure is intended for skilled system programmers who have experience with the z/OS systems that are monitored clients.

Before you begin

- Make sure that your installation has completed the procedures in:
 - Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79.
 - Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91.
- Identify the z/OS system from which you plan to send priming data to the IBM zAware server, and make sure that you configure this priming system according to the instructions in Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91.
- List the systems for which you plan to send priming data; the location, names, and sizes of the sequential data sets that contain their priming data; and the order in which you want to send priming data. These systems must be configured as described in Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91 before you send their priming data.

The recommended approach is to transfer only a portion of the priming data for a monoplex or sysplex to verify the configuration of the IBM zAware environment. When the transfer is successful, you can transfer the remaining data for one monoplex or sysplex at a time. If you transfer priming data for multiple sysplexes through one invocation of the REXX exec, priming data for some systems can be overlaid.

- To configure and run the z/OS bulk load client for IBM zAware on the priming z/OS system, the user ID under which the z/OS bulk load client runs must have authority to use log streams. The z/OS bulk load client can process sequential data sets that contain only SYSLOG data that is stored in hardcopy log 2-digit year (HCL) or 4-digit year (HCR) format.

To use the z/OS bulk load client, you also need to check and modify storage attributes for the log stream that it uses. See *z/OS DFSMSdfp Storage Administration* if you need additional details about creating SMS classes and other related DASD storage attributes for the log stream.

- To log in to the IBM zAware graphical user interface (GUI), you need to know the URL.

The URL includes the IP address or host name assigned to the IBM zAware partition:

`https://ip_address/zAware/` or `https://host_name/zAware/`

The “zAware” portion of the URL is case-sensitive.

To assign priming data and use it to create the model of system behavior, you use specific administration functions in the IBM zAware GUI. To use these functions, you must log in to the GUI with a user ID that is assigned to the Administrator role.

About this task

After your installation completes the procedure in Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91, the IBM zAware server is receiving current data from the z/OS system logger running on z/OS monitored clients. However, the server cannot use this data for analysis until a model of normal system behavior exists. The estimated amount of data for building the most accurate models is 90 days of data for each client. Your installation can modify the number of days required for this training period, based on your knowledge of the workloads running on z/OS monitored clients. This training period applies for all monitored clients; you cannot define a different training period for each client. Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79 contains information about the training period for analytics.

Instead of waiting for the IBM zAware server to collect data over the course of the training period, you can prime the server by transferring prior data from the hardcopy or system logs of monitored clients, and request the server to build a model for each client from the transferred data. To transfer this priming data, you configure a log stream and run the z/OS bulk load client through a REXX exec on a z/OS system. You can run the REXX exec for the z/OS bulk load client in the TSO/E foreground or in the background as a batch job. This procedure explains how to run the exec as a batch job after editing sample JCL in SYS1.SAMPLIB.

Through the z/OS bulk load client, you can transfer data for one or more monitored clients by identifying the sequential data sets that contain the priming data. If any data set has been archived, the z/OS bulk load client can recall the data set, transfer its contents, and migrate the data set.

The process of transferring priming data could require several hours or more, depending on a number of factors that include:

- The priority of the job that runs the REXX EXEC for the z/OS bulk load client
- The amount of priming data to be sent, and whether any of that priming data resides on migrated data sets
- The network configuration and traffic at your installation

For example, if you run the REXX EXEC at a very high priority to send 46000 tracks of priming data that is archived, the transfer might take approximately 10 to 15 minutes. The process can take longer if the z/OS bulk load client runs at a lower priority, or if network or system conditions are not favorable when the REXX EXEC runs.

In contrast to data that the IBM zAware server receives from the z/OS system logger running on a monitored client, the priming data from the z/OS bulk load client does not include the name of the sysplex to which the monitored client belongs. Without the sysplex name, the IBM zAware server cannot associate the priming data with the appropriate sysplex. You use the **Administration > Configuration > Priming Data** page in the IBM zAware GUI to assign the received priming data to the appropriate sysplex. After the priming data is associated with the appropriate sysplex, you can request the IBM zAware server to build the model.

To build the model for a specific monitored client, you have two options:

- You can use the **Request Training** action on the **Administration > Training Sets** page. Any data that the z/OS system logger is currently sending does not become part of the model for the client until you request training again or the IBM zAware server automatically rebuilds the model. This priming option is recommended because analysis can start shortly after the model is built.
- You can wait for the next scheduled training, during which the IBM zAware server automatically uses the priming data to build the model. In this case, any data that the z/OS system logger is currently sending becomes part of the model for the client.

The time required for an automatic or manual training request to complete depends on the amount of priming data that the bulk loader sent; typically, the training process takes only several minutes to complete but might take longer for large amounts of priming data. After the training status shown on the

Training Sets page changes from “In progress” to “Complete”, a model containing the priming data is available for the IBM zAware server to use for analysis, when the client is connected and sending current data.

Procedure

1. On the z/OS system from which you plan to send priming data, configure the z/OS bulk load client. The z/OS bulk load client load modules reside in SYS1.MIGLIB and sample files reside in SYS1.SAMPLIB.
 - a. Decide where you want the z/OS bulk load client load modules to reside. You have the option to copy the AIZBLKR and AIZBLKM load modules from SYS1.MIGLIB into an authorized or unauthorized library. If you decide to leave the load modules in SYS1.MIGLIB, however, make sure that you either add SYS1.MIGLIB to the LINKLIST concatenation or to the JCL JOBLIB or STEPLIB parameter for the job that runs the REXX exec.
 - b. Copy the z/OS bulk load client sample files from SYS1.SAMPLIB into your JCL library.
 - 1) Copy AIZBLK to a JCL data set. AIZBLK contains a sample job that completes the following steps:
 - a) Defines a model log stream to establish the attributes of the target log stream that the z/OS bulk load client creates and uses for priming data. The z/OS bulk load client writes priming data into this target log stream.
 - b) Defines and populates a control data set that lists the sequential data sets containing priming data to be transferred.
 - c) Invokes the z/OS bulk load client to transfer the priming data.
 - d) Deletes the model log stream and the target log stream that was used to send the priming data.
 - 2) Copy AIZBLKE from SYS1.SAMPLIB to a data set in your SYSEXEC concatenation. AIZBLKE contains the sample REXX exec to run the AIZBLKR load module.
If the target data set is VB format, make sure the numbers in columns 72-80 are deleted before you copy AIZBLKE into the data set.
 - c. For the sequential data sets that contain priming data, check the following values.
 - If the priming data contains ANSI carriage control characters, check that the RECFM attribute of the data set indicates ANSI control characters, such as VBA or FBA.
 - If the priming data contains machine control characters, check that the RECFM attribute of the data set indicates machine control characters, such as VBM or FBM.
 - d. Check the g.MaxImportBytes value in the AIZBLKE REXX exec. This value controls the maximum amount of data that can be imported per job. You might need to change this value to accommodate the amount of priming data that you plan to send to the IBM zAware server.
 - e. Modify the sample JCL according to the customization instructions in the AIZBLK file. To run the REXX exec as a batch job, you need to modify the sample JCL. Make sure that you make the following changes:
 - Check the value set for the REGION parameter; depending on the amount of data you are sending, you might need to specify REGION=0M on the step for running the REXX exec.
 - Update the model log stream name to match naming standards at your installation.
 - Check the logger keywords and parameters as noted in the following list. For more information, see the topic about LOGR keywords and parameters for the administrative data utility in z/OS *MVS Setting Up a Sysplex*, SA22-7625.
 - Check the parameters that control the use of offload data sets and, if necessary, modify the values to match the following code sample:

```
AUTODELETE(YES)
HIGHOFFLOAD(60)
LOWOFFLOAD(30)
```
 - Check that the DFSMS data classes for staging data sets and offload data sets are set to the recommended control interval (CI) sizes. In the following statements, the LOGR4K and

LOGR24K values are sample data class names; substitute the appropriate data class names that are defined in the DFSMS configuration for your installation.

STG_DATACLAS(LOGR4K)
LS_DATACLAS(LOGR24K)

- Check the LS_SIZE and STG_SIZE parameters to ensure that they are set to reasonable values, based on the amount of priming data you are sending. If the size of the log stream data sets are established through DFSMS data class definitions, you can omit the LS_SIZE and STG_SIZE parameters.

LS_SIZE(size)

Specifies the size, in 4K blocks, of the log stream offload DASD data sets for the log stream being defined.

STG_SIZE(size)

Specifies the size, in 4K blocks, of the DASD staging data set for the log stream being defined.

Keep in mind that the recommended approach is to complete the following tasks in sequence; these tasks determine which data sets you select for the first invocation of the z/OS bulk load client.

- 1) Transfer only a portion of the priming data for a monoplex or sysplex to verify the configuration of the IBM zAware environment.
 - 2) When you verify that the transfer was successful, transfer the remaining data for one monoplex or sysplex at a time. If you transfer priming data for multiple sysplexes through one invocation of the REXX exec, priming data for some systems can be overlaid.
- f. Update security definitions to allow the z/OS bulk load client to access the log stream and the data sets that contain priming data. The z/OS bulk load client requires the following authorization through the z/OS Security Server (RACF), or an equivalent security product:
- UPDATE access for the log stream
 - READ access for the priming data sets
- g. Check the connection between the priming z/OS system and the IBM zAware server. Issue the following MVS command:

```
DISPLAY LOGGER,STATUS,ZAI,VERIFY
```

The system responds with message IXG601I; the following sample illustrates the message display.

```
SYSTEM LOGGER STATUS
SYSTEM  SYSTEM LOGGER STATUS
-----
SY1     ACTIVE
```

```
ZAI LOGSTREAM CLIENTS: AVAILABLE
BUFFERS IN USE: 00 GB 0000 MB
ZAI VERIFY INITIATED, CHECK FOR MESSAGES IXG37X, IXG38X
```

```
LOGGER PARAMETER OPTIONS
KEYWORD          SOURCE    VALUE
-----
ZAI
SERVER           IPL (NN)  HOST.ZAWARE.SERVER.LOCATION
PORT             DEFAULT   2001
LOGBUFMAX        DEFAULT   02
LOGBUFWARN       DEFAULT   75
LOGBUFFULL       DEFAULT   MSG
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR DISPLAY ZAI,VERIFY
STATUS:  ATTEMPTING SOCKET CREATE
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR DISPLAY ZAI,VERIFY
STATUS:  SOCKET CREATE SUCCESSFUL
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR DISPLAY ZAI,VERIFY
STATUS:  ATTEMPTING SOCKET CONNECT
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR DISPLAY ZAI,VERIFY
```

```

STATUS: SOCKET CONNECT SUCCESSFUL
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR DISPLAY ZAI,VERIFY
STATUS: INITIATING SOCKET VALIDATION
IXG386I ZAI LOGSTREAM CLIENT CONNECT ATTEMPT IN PROGRESS FOR DISPLAY ZAI,VERIFY
STATUS: SOCKET VALIDATION SUCCESSFUL

```

```

IXG380I ZAI LOGSTREAM CLIENT ESTABLISHED
FOR DISPLAY ZAI,VERIFY

```

2. On the priming z/OS system, run the z/OS bulk load client to send priming data to the IBM zAware server.
 - a. Submit the edited JCL sample for processing. The time required for the z/OS bulk load client to transfer the priming data depends on how much data is in the data sets listed in the control file. If a data set has been archived, the transfer process requires more time for the z/OS bulk load client to recall the data set, transfer its contents, and migrate the data set.

When the job completes, check the job log for the return code from the z/OS bulk load client.

Possible return code values are:

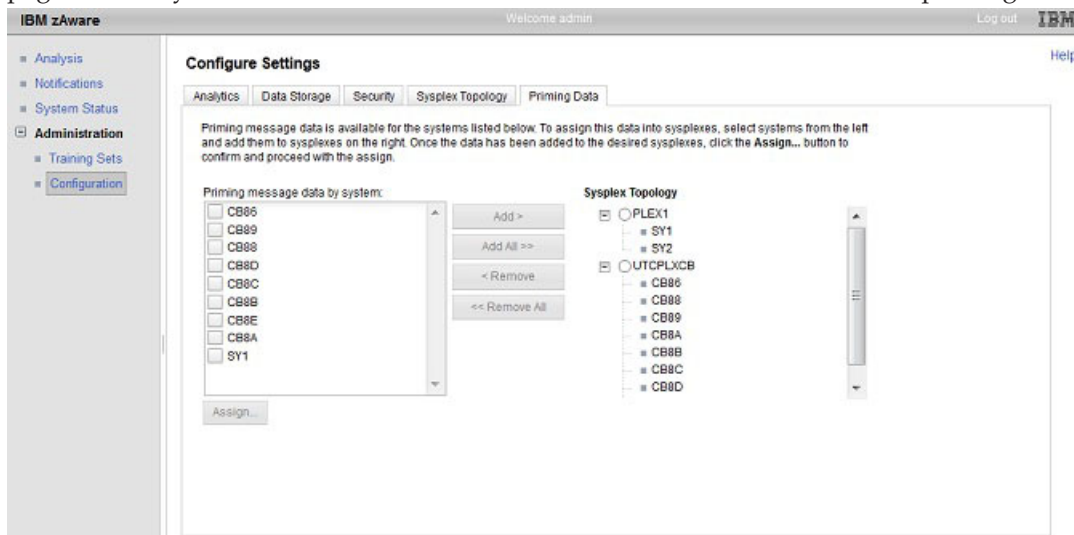
```

0      Successful
4      Request not valid
8      Request failed

```

A return code of 0 indicates that the priming data is queued for transmission to the IBM zAware server.

- b. Check for an indication that the z/OS system logger sent the priming data. Look in the system log (SYSLOG) for IXG38x or IXG37x messages that report problems with the transfer of data between the z/OS system logger and the IBM zAware server.
- c. Verify that the IBM zAware server has received the priming data. Through the IBM zAware GUI, check the **Priming data by systems** list on the **Administration > Configuration > Priming Data** page for the system name of the z/OS monitored client associated with the priming data.



- d. Edit and resubmit the JCL, as necessary, to finish sending the priming data for the z/OS monitored clients.
3. Through the IBM zAware GUI, assign the received priming data to the appropriate sysplex. After the data transfer from the priming z/OS system is complete, the IBM zAware server indicates the data received by adding the system name in the **Priming data by systems** list on the **Administration > Configuration > Priming Data** page. The system name is the name of the z/OS monitored client associated with the priming data. Because the z/OS bulk load client can send data for more than one monitored client at a time, several systems might be listed.

The following steps explain how to assign priming data from monitored clients (systems) by moving those systems from the **Priming data by systems** list to the **Sysplex Topology** list on the **Priming**

Data page. You do not have to assign all systems in the list until you are ready to do so. Unassigned systems remain in the **Priming data by systems** list until you add them to the sysplex topology.

- a. In the **Sysplex Topology** list, select the sysplex to which you want to assign systems.
- b. In the **Priming data by systems** list, select the systems that you want to move to the selected sysplex and click **Add >**. If you want to assign all of the systems in the **Priming data by systems** list to the same sysplex, you do not have to select them first; instead, you can use **Add All >>** to move all systems in the list to the selected sysplex. After you click **Add >** or **Add All >>**, the systems are moved from the **Priming data by systems** list to the **Sysplex Topology** list. They are displayed under the selected sysplex, with the parenthetical phrase “data to be assigned” displayed after the system name. If necessary, expand the sysplex topology to see the list of systems for the selected sysplex.
- c. As necessary, repeat steps a and b to move each system in the **Priming data by systems** list to the appropriate sysplex in the **Sysplex Topology** list.
- d. When you have finished moving systems from the **Priming data by systems** list to the appropriate sysplex, click **Assign** to apply your changes.
- e. Review and confirm your changes by clicking **OK** on the **Assign Priming Data** window.

IBM zAware assigns the priming data to the appropriate sysplex. During this process, IBM zAware recycles its analytics engine. When the analytics engine is stopped or recycled, IBM zAware disconnects all monitored systems from the server. When z/OS monitored clients are disconnected from the server, they automatically attempt to reconnect and continue to buffer data for approximately 10 minutes. If the analytics engine is restarted within that time, the z/OS system reconnects and sends the buffered data to the IBM zAware server. If the z/OS system times out before the analytics engine is restarted, any buffered data is lost and you must manually reconnect the system. To reconnect a z/OS system, you must issue the SETLOGR command.

SETLOGR FORCE, ZAICONNECT, LSN=SYSPLEX.OPERLOG

4. Verify that the transferred data is available for the IBM zAware server to use.
 - a. From the **Administration > Training Sets** page, select the system name of the z/OS monitored client.

Training Sets

Help

The Monitored Systems table provides training statuses and results for IBM zAware monitored systems. The Actions menu provides functions for managing model dates, requesting or canceling training, and managing ignored messages. Training details for a given system can be accessed by clicking on links in the Training Progress and Last Training Result columns.

Monitored Systems

| System | Sysplex | Training Progress | Last Training Result | Last Training Result Time | Current Model Built |
|--------|----------|-------------------|----------------------|--|--|
| SY1 | PLEX1 | — | Failed | August 30, 2012 2:32:26 PM Eastern Daylight Time | August 30, 2012 2:31:15 PM Eastern Daylight Time |
| SY2 | PLEX1 | — | Complete | August 30, 2012 5:05:04 PM Eastern Daylight Time | August 30, 2012 5:05:04 PM Eastern Daylight Time |
| CB85 | UTCPLXCB | — | Never Connected | — | — |
| CB88 | UTCPLXCB | — | Never Connected | — | — |
| CB89 | UTCPLXCB | — | Never Connected | — | — |
| CB8A | UTCPLXCB | — | Never Connected | — | — |
| CB8B | UTCPLXCB | — | Never Connected | — | — |
| CB8C | UTCPLXCB | — | Never Connected | — | — |
| CB8N | UTCPLXCB | — | Never Connected | — | — |

Current Training Status Details (Click on training statuses above to view details)

| | | |
|--|--------------------------------------|--|
| System name: SY1 | Training progress: — | Last training result: Failed |
| Training start time: August 30, 2012 2:32:23 PM Eastern Daylight Time | Time in training(h:m:s): 00:00:02 | Last training result time: August 30, 2012 2:32:26 PM Eastern Daylight Time |
| Entered queue time: August 30, 2012 2:32:23 PM Eastern Daylight Time | Time in queue(h:m:s): 00:00:00 | |

Refresh Last Refresh: Thu Aug 30 2012 17:21:17 GMT-0400 (Eastern Daylight Time)

- b. From the **Actions** list, select **Manage Model Dates**.

- c. From the **Manage Model Dates** page, select **Next Training Period Model Dates** from the **Model dates** list.

Use the calendar view to determine days for which transferred data is available. Calendar days that are not marked as “Excluded” or “Unavailable” identify the dates for which the IBM zAware server has data to use.

Training Sets > Manage Model Dates

Manage Model Dates

Model dates for the selected system are displayed in the calendar. To switch between *Current Model Dates* and *Next Training Period Model Dates*, use the ‘Model dates’ selector. When displaying *Next Training Period Model Dates*, days can be included or excluded from future training periods by clicking on them or selecting a date and hitting Enter.

Training System:
UTCPLXCB.CB8E

Model dates:
Next Training Period Model Dates ▼

Switch to Summary View

Training calendar (UTC):



Return to Training Sets

- d. Click **Return to Training Sets** to return to the previous page.
 - e. Repeat these steps, as necessary, for each system for which data was transferred.
5. Optional: Request the IBM zAware server to build models from the priming data. Otherwise, you can wait for the next scheduled training and the IBM zAware server automatically uses the priming data when it builds the model. To check the dates for the training period, use the instructions in What to do next.

- a. Through the **Administration > Training Sets** page, select one monitored client (system).
- b. From the **Actions** list, select **Request Training** to build a model for the selected client.
- c. Confirm your request by clicking **OK** on the **Request Training** window. On the **Administration > Training Sets** page, the **Current Training Status** column for the monitored client (system) that you selected contains either “In Progress” or “In Queue”, with the queue position indicated.
- d. Repeat these steps, as necessary, for each system for which priming data was transferred.

The time required for the training request to complete depends on the amount of priming data that the bulk loader sent; the training process might take several hours to complete. To track progress, use any of the following techniques.

- Click **Refresh** to update the **Training Sets** page content.
- Click ► to expand the **Current Training Status Details** section, then click on any value in the **Current Training Status** column to view details.

For an explanation of the **Training Sets** page content, see “Training Sets page” on page 166.

Results

After the training process completes for a given client (system), a model containing the priming data is available for the IBM zAware server to use for analysis, when the client is connected and sending current data.

What to do next

View current analysis data for monitored clients as described in Chapter 14, “Viewing and using analytical data to monitor and diagnose system behavior,” on page 109.

Part 4. Managing and using the IBM zAware server

Topics in this part describe the IBM zAware GUI functions that systems programmers, systems administrators, and experienced application programmers use for daily operations, which include viewing and analyzing data from monitored clients. Additional topics include management tasks for modifying the IBM zAware resources or operations.

Topics covered in this part are:

- Chapter 14, “Viewing and using analytical data to monitor and diagnose system behavior,” on page 109
- Chapter 15, “Specifying security settings for the IBM zAware GUI,” on page 129
- Chapter 16, “Managing IBM zAware operation and resources,” on page 143

Chapter 14. Viewing and using analytical data to monitor and diagnose system behavior

Through the IBM zAware graphical user interface (GUI), you can view analytical data that indicates which system is experiencing deviations in behavior, when these anomalies occurred, and details about unusual messages and unusual message patterns. Using this information, you can take corrective action for these anomalies before they develop into more visible problems.

In the IBM zAware GUI, information in the **Analysis** page and **Interval view** can help you find and diagnose anomalies in at least three situations:

- When a problem occurs
- After a change has been made
- When a random problem occurs intermittently

The following topics provide descriptions of the **Analysis** page and **Interval view** and explain how to use the information in these pages to diagnose different types of anomalies:

- “Using the Analysis page to monitor and diagnose system behavior”
- “Using the Interval view to pinpoint the causes of system anomalies” on page 118

The final topic, “Verifying planned system changes with IBM zAware” on page 127, describes how to use IBM zAware for purposes other than problem diagnosis.

These topics describe only key elements of pages in the IBM zAware GUI. For descriptions of GUI page elements, see the online help.

Using the Analysis page to monitor and diagnose system behavior

You can use the Analysis page provided in IBM zAware to help you determine which monitored system is behaving abnormally, the time when the abnormal behavior occurred, and how many unique messages were issued at that time.

To display the Analysis page, click **Analysis** in the navigation pane. The default presentation of the Analysis page is a graphical view bar graphs that provide a clear visual indication of the time when abnormal behavior occurred and how many unique messages were issued at that time. This analytical data is also available in an equivalent tabular format.

The Analysis page is blank until the following prerequisites are satisfied:

- At least one storage device has been added to the **Administration > Configuration > Data Storage** tab for IBM zAware to use for storing analysis results, system behavior models, and data from monitored clients (systems).
- At least one z/OS system is connected to the IBM zAware server and is transferring its current SYSLOG or OPERLOG data to the server.
- IBM zAware has created a model of normal behavior for the system.

Your installation has two options for building the IBM zAware models for monitored clients:

- You can prime the server by transferring prior data for monitored clients, and request the server to build a model for each client from the transferred data. This priming option is recommended because analysis can start shortly after the model is built.
- You can wait for the server to collect the required amount of data for each connected client. This data requirement is known as the *training period* for IBM zAware analytics. When the server receives data from a client for the duration of the training period, the server automatically builds the model.

Chapter 8, “Planning to create IBM zAware models,” on page 57 provides information about building models to accurately reflect normal system behavior. Ideally, the model represents a predictable, stable workload that generates the same artifacts when the monitored client, its subsystems, hardware, and applications are working as your installation expects them to function. Through its pattern recognition techniques and the process of building the model, which is called *training*, the IBM zAware server learns about the typical behavior of a specific system and its workload.

Once a model exists for a monitored client and that client is connected and sending current data to the IBM zAware server, the server can compare current data to the model to determine interval anomaly scores.

Understanding interval anomaly scores

An *interval anomaly score* indicates the relative difference in behavior of the monitored system, as compared to the system model. To determine system anomaly scores for a given system, the IBM zAware server must have a model of normal system behavior to compare with current data it is receiving from that system.

For each 10-minute interval during a specific date and time period, the IBM zAware server constructs an interval anomaly score and unique message ID count for each connected client that is sending current data. For each client, the server compares message patterns in the current data to the model for that client. The server displays interval anomaly scores and unique message ID counts in a bar graph that contains one rectangle for each 10-minute interval, as shown in Figure 30. This analytical data is also available in an equivalent tabular format.

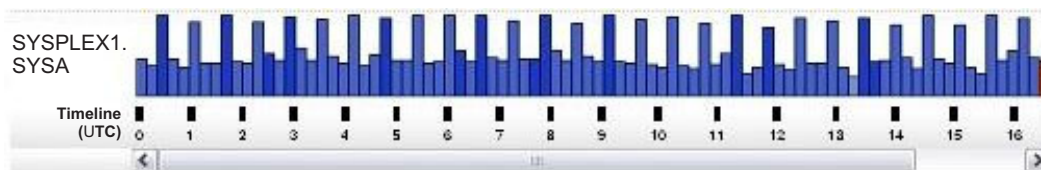


Figure 30. A sample bar graph from the **Analysis** page display

The interval anomaly score indicates the difference in current behavior compared to the expected behavior that is reflected in the client model. If the interval contains messages that are relatively normal, common messages for that client, the server assigns a low score and light blue color to the interval. For example, suppose that you have configured a relatively stable test system as a IBM zAware monitored client. On this test system, various subsystems, such as Customer Information Control System (CICS®) and WebSphere MQ, are recycled on a regular basis. This behavioral pattern is reflected in the client model that the server uses for analysis. When a current subsystem recycle completes normally, the intervals for subsystem recycling receive a low interval anomaly score and light blue color, because the pattern of messages issued during a successful recycle match an expected behavior in the model. However, if any unexpected messages are issued during a current subsystem recycle, the IBM zAware server assigns a higher interval anomaly score and darker blue, gold, or orange color to those intervals that contain the unexpected or unique messages.

The IBM zAware server uses unsupervised machine learning and IBM rules to determine interval anomaly scores for all monitored clients.

- Through *unsupervised machine learning*, the IBM zAware server extracts and organizes message data to build a model of behavior for each monitored client. This training process is repeated over time, with the frequency determined by the training interval, which enables the server to update and refine each client model.
 - Through the training process, the IBM zAware server determines which messages are issued during routine system events, such as starting a batch job or a particular subsystem. For such system

events, the server identifies and recognizes the pattern of messages that are associated with each event. The message patterns are called *clusters* and define the normal context for the messages in the cluster.

When the server detects a specific message that is issued outside of its expected context (that is, without the other messages in the cluster), the server assigns a higher interval anomaly score and darkest blue, gold, or orange color to the interval that contains the message.

- Also through the training process, IBM zAware determines the distribution of each unique message ID within a collection of intervals in the message data used for training. This distribution influences the interval anomaly score that the IBM zAware server displays for an interval of current data from the client. For clients that exhibit relatively stable behavior, only a small change causes the server to assign a higher interval anomaly score; for relatively unstable clients, larger changes are required before the server assigns a higher anomaly score to a given interval.

In summary, through the training process, the server learns about expected message patterns (clustering) and interval anomaly scores, and stores this information as part of the model for a specific client. IBM zAware uses this model data to determine interval scores when it analyzes current data that it receives from the client.

- z/OS experts at IBM know, based on decades of IBM experience with testing and using z/OS systems, which message IDs are likely to indicate potential problems. Message IXC101I, for example, indicates that a system is being removed from a sysplex. For a test system, this removal process could be reflected in the IBM zAware model for this system as a normal, expected behavior pattern. In the analytical data for this test system, you might expect the server to assign a low anomaly score and light blue color to any intervals that contain such a system removal, when message IXC101I is issued in context.

However, message IXC101I might indicate a potential problem, whether or not it is issued in context. Because the removal of a system from a sysplex warrants further investigation, the IBM zAware server is programmed to assign the highest interval anomaly score and orange color to intervals in which message IXC101I is issued. This rule for IXC101I and IBM rules for other known messages contribute to the interval anomaly score.

In summary, comparison to the model, context, and IBM rules are key factors that contribute to the interval anomaly scores for systems in the **Analysis** page display.

The possible interval anomaly scores are:

0 through 99.4

The interval contains messages and message clusters that match or exhibit relatively insignificant differences in expected behavior, as defined in the IBM zAware model. A score of 0 is possible because the server eliminates all expected, in-context messages from its scoring calculation. A score of 0 indicates intervals that exhibit no difference in behavior compared to the system model. In the bar graph display, these intervals are colored with the lightest blue shade.

Intervals with scores that are greater than 0 but less than 99.5 contain some messages that are unexpected or issued out of context. Scores in this range indicate intervals that do not vary significantly from the system model. In the bar graph display, these intervals are colored with varying shades of blue.

- 99.5** Intervals with this score contain some rarely seen, unexpected, or out-of-context messages. Generally speaking, this score indicates intervals with some differences from the system model but do not contain messages of much diagnostic value. In the bar graph display, these intervals are colored with the darkest blue shade.

99.6 - 100

Intervals with this score contain rarely seen messages (these messages appear in the model only once or twice), or many messages that are unexpected or issued out of context. This score indicates intervals with more differences from the system model; these intervals can contain messages that might help you diagnose anomalous system behavior. In the bar graph display, these intervals are the color gold.

- 101 Intervals with this score exhibit the most significant differences from the system model; these intervals contain messages that merit investigation. In the bar graph display, these intervals are the color orange. IBM zAware assigns this score to intervals that contain:
- Unique message IDs that the server has not detected previously in the client model
 - Unusual or unexpected messages
 - Messages that IBM rules define as critical
 - A much higher volume of messages than expected

Analysis page controls and content

When you select the **Analysis** page in the IBM zAware GUI, the display contains interval anomaly scores for the monitored clients that are connected to the IBM zAware server. Figure 31 illustrates a sample of the default graphical display with systems from PLEX1.

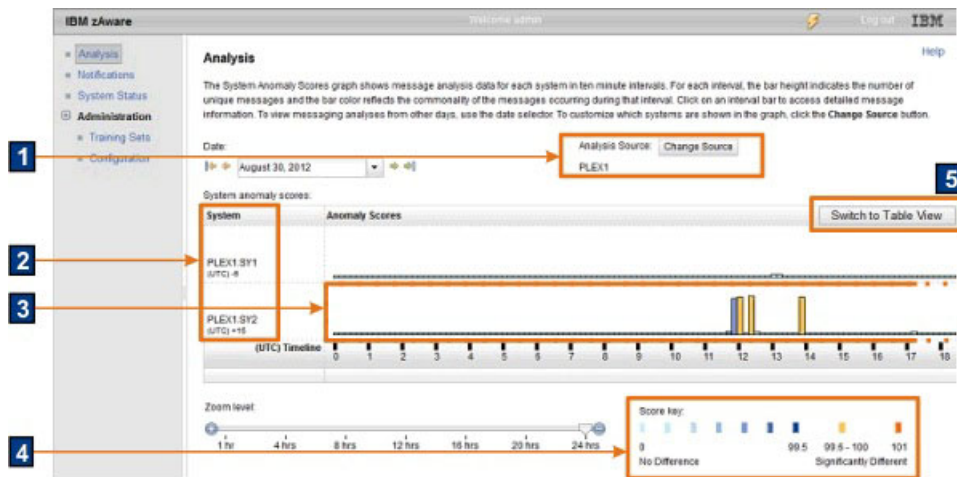


Figure 31. A sample **Analysis** page

1. The **Analysis Source** field identifies whether the display on this page includes all monitored systems, only the systems in a specific sysplex, or only specific systems. By default, all connected systems are displayed in the **Analysis** page. You can click **Change Source** to modify which systems are presented in the display.

Depending on the number of connected systems at your installation, the IBM zAware GUI might require some time to render the initial **Analysis** page display. For better performance, use **Change Source** to filter the display by sysplex or a selected set of systems. This filter setting remains in effect for the duration of the browser session or until you use **Change Source** to modify it.

2. The **System** column displays the names of the z/OS systems running in the local CPC or in a specific sysplex. The name has the format *sysplex-name.system-name*, where *sysplex-name* is the name of the sysplex to which the system belongs and *system-name* is the name of the system. The UTC offset for the time zone in which the system resides follows the system name.

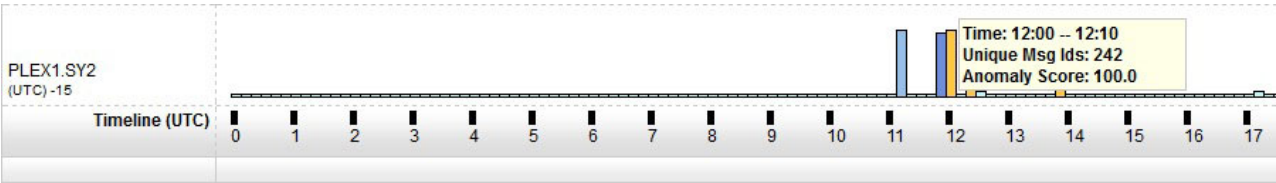
You might need to scroll this list depending on the number of systems.

3. For each system, the **Anomaly Scores** column displays a bar graph that contains one rectangle for each 10-minute interval during a specific UTC date and time period. The server builds this analytical data by comparing current data from each client to the model for that client. This analytical data is also available in an equivalent tabular format.

The analytical data in the **Anomaly Scores** column is refreshed automatically, every two minutes. For the most recent 10-minute interval, the rectangle representing that interval is redrawn as the server refreshes the display with more up-to-date analytical data.

For additional details about a given interval, you can position your cursor over a rectangle to display the exact time of the interval, the number of unique message IDs issued during that interval, and the

exact anomaly score.



If you want additional details about an interval of diagnostic interest, click the rectangle to open the **Interval view**.

4. The **Interval anomaly score key** correlates the color of an interval in the bar graph to its relative anomaly score. The interval anomaly score indicates unusual patterns of message IDs within a given interval, as compared to the model of normal system behavior for a specific system.



The interval anomaly scores range from 0 to 101. A score of 0 means that the IBM zAware server detected no difference from the system model for the interval; the interval contains expected messages and message clusters that match the model. A score of 101 means that the server detected significant differences from the system model; the interval contains one or more new messages or many messages issued out of context. The server also assigns a score of 101 for the following conditions:

- The interval contains one or more messages that IBM rules define as a critical message.
- The interval receives an anomaly score that is greater than twice the largest interval score in the model.

Intervals with lower scores are colored with varying shades of blue. Intervals with higher scores are colored with the darkest shade of blue, or with gold or orange.

5. Through **Switch to Table View**, you can view IBM zAware analytical data in a tabular rather than graphical format. For a description of the tabular view, see “The Analysis page in tabular format” on page 117.

Figure 32 on page 114 highlights the controls that you can use to modify the date and time for the display on the **Analysis** page.

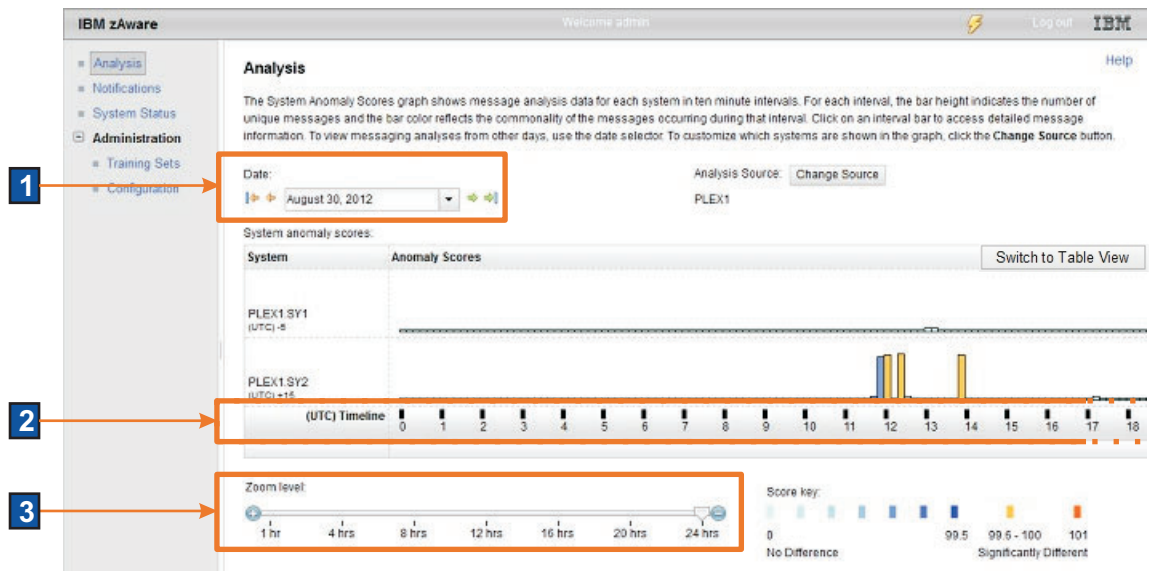


Figure 32. Date and time controls for the **Analysis** page

1. The **Date** field displays the currently selected Coordinated Universal Time (UTC) date. You can change the current day to another date.
2. The **Timeline** marks the hours of the day in UTC, using the 24-hour clock. You can move the slider to display hours that do not show in the **Analysis** page. For a sysplex that contains systems that operate in different time zones, IBM zAware converts the times to UTC times to align the current times across monitored systems.
3. The **Zoom level** slider controls how many hours of the day are displayed in the **Analysis** page. You can move the slider to display all hours or only a few hours.

Using the **Timeline** and **Zoom level** together, you can change the display to focus on anomaly scores in a specific period.

■ Tips for using the graphical **Analysis** page

The bar graphs in the **Anomaly Scores** display provide a clear visual indication of anomalous behavior through the height or color of interval rectangles. To find intervals that merit investigation, use the following tips.

- Color is the primary indicator of anomalous behavior, so look for dark blue, gold, or orange rectangles. The height of the rectangle is an additional indicator of unusual activity, with taller rectangles indicating a higher number of unique messages.

Depending on the initial display on the **Analysis** page, you might need to use various controls to find these rectangles:

- Use **Change Source** to modify which systems are presented in the display.
- Use the scroll bar, if one is displayed, to view all systems in the list.
- Use the date and time controls to focus on a specific time period.

Depending on the number of connected systems at your installation, the IBM zAware GUI might require some time to render the initial **Analysis** page display. For better performance, use **Change Source** to filter the display by sysplex or a selected set of systems. This filter setting remains in effect for the duration of the browser session or until you use **Change Source** to modify it.

Depending on the number of connected systems at your installation, the IBM zAware GUI might require some time to render the initial **Analysis** page display. For better performance, use **Change Source** to filter the display by sysplex or a selected set of systems. This filter setting remains in effect for the duration of the browser session or until you use **Change Source** to modify it.

When you select **Change Source**, the IBM zAware server displays the Change Analysis Source window, as illustrated in Figure 33.

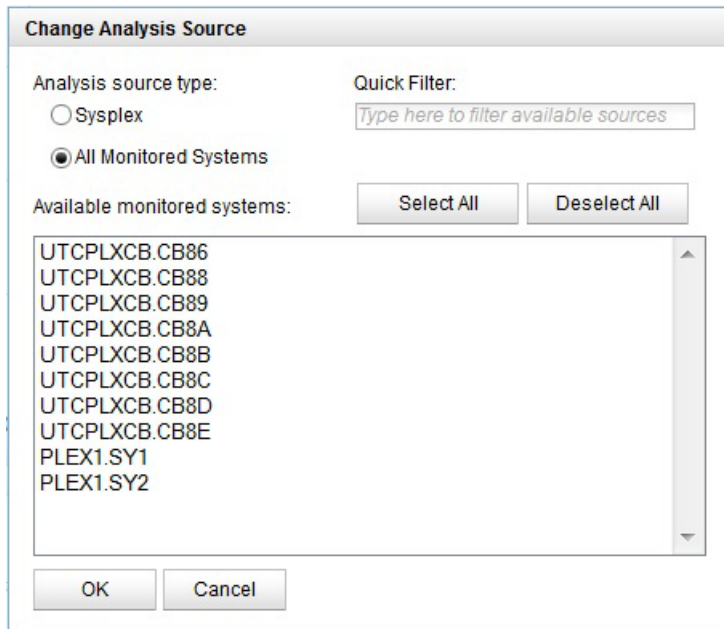


Figure 33. A sample Change Analysis Source window

- I For a description of the Change Analysis Source window, see “Change Analysis Source window.”
- When you find intervals of diagnostic interest, position your cursor over each rectangle to display the exact time of the interval, the number of unique message IDs issued during that interval, and the exact interval anomaly score. Investigate intervals with the following characteristics:
 - An interval anomaly score of 101. These intervals are represented by orange rectangles.
 - Multiple intervals with an interval anomaly score of 101.
 - A significant change in interval anomaly score from one interval to the next.
 - One of the following height and color combinations:
 - Short and dark-colored rectangles are interesting.
 - Tall and light rectangles can be interesting.
 - Intervals with no data are interesting.

Also check prior intervals, which might yield additional information. Depending on the type of workload your installation runs on z/OS, checking the system behavior on prior days (for example, the day before or the same day last week) might be helpful as well.

- Although the **Analysis** page display is useful for finding unexpected problems or reported incidents, you also can use it to verify behavior after a planned change. For additional information, see “Verifying planned system changes with IBM zAware” on page 127.

Change Analysis Source window

You can use the Change Analysis Source window provided in IBM zAware to change the systems listed in the display on the Analysis page. By default, all monitored systems are displayed on the Analysis page but you can modify the display to show systems in a specific sysplex or to show only specific systems.

To display the Change Analysis Source window, click **Analysis** in the navigation pane. Then, click **Change Source** in the **Analysis source** field on the Analysis page.

For a description of the fields that are displayed in the Analysis Source window, see Table 24 on page 116.

Notes about the availability of analytical data

- Analytical data might not be available for all systems for the date and time that you select for the Analysis page display. Data is not available under the following circumstances:
 - The monitored client is not connected and sending current data to the IBM zAware server.
 - The monitored client was added to the sysplex topology after the date you select for the Analysis page display.
- Analytical data is also not available for the dates for which you supplied priming data, unless the monitored client was connected and sending data to the IBM zAware server on those dates. The server uses priming data only for creating the model of system behavior.

Fields in the Change Analysis Source window

Table 24 describes the fields that are displayed in the Change Analysis Source window.

Table 24. Fields in the Change Analysis Source window

| Field | Description |
|-----------------------------|---|
| Analysis source type | <p>Controls the content that is displayed in the Available monitored systems list and the Available sysplex sources list. Select one of the following options:</p> <p>Sysplex Displays the Available sysplex sources list, and populates the list with the names of the sysplexes that currently exist in your sysplex topology. Select this option to include all the monitored systems that belong to a specific sysplex in the Analysis display.</p> <p>All Monitored Systems Displays the Available monitored systems list, and populates the list with the names of all the monitored systems that currently exist in your sysplex topology. Select this option to include all or a subset of the monitored systems in the Analysis display. This option is selected by default.</p> |
| Available sysplex sources | <p>Lists the name of the sysplexes that currently exist in your sysplex topology.</p> <p>This field is displayed only if you select Sysplex in the Analysis source type field. If displayed, select one or more sysplexes. To select more than one sysplex, press Ctrl and click the sysplex names. If you do not select any sysplexes and you click OK, all of the sysplexes are included in the resulting display.</p> |
| Available monitored systems | <p>Lists the name of the monitored systems that currently exist in your sysplex topology. The name has the format <i>sysplex-name.system-name</i>, where <i>sysplex-name</i> is the name of the sysplex to which the system belongs and <i>system-name</i> is the name of the system.</p> <p>This field is displayed only if you select All Monitored Systems in the Analysis source type field. If displayed, select one or more systems to include in the display on the Analysis page. To select more than one system, press Ctrl and click the system names. If you do not select any systems and you click OK, all of the systems are included in the resulting display.</p> |
| Quick filter | <p>Allows you to filter the Available monitored systems list or the Available sysplex sources list so that you can quickly locate the system or sysplex that you want to select.</p> <p>To find a specific sysplex, type the first few characters of the sysplex name. To find a specific system, type the sysplex name followed by a period and the first few characters of the system name; for example: SYSPLEX1.SYS</p> <p>If a match exists in the list, the list scrolls to the name of the sysplex or system that starts with the characters you entered.</p> |

The Analysis page in tabular format

The tabular view of the Analysis page is provided to improve the accessibility of IBM zAware data. To display the tabular view, click **Switch to Table View** on the toolbar of the Interval Anomaly Scores by System table on the default graphical Analysis page.

Figure 34 provides a sample illustration of the **Analysis** page in tabular format.

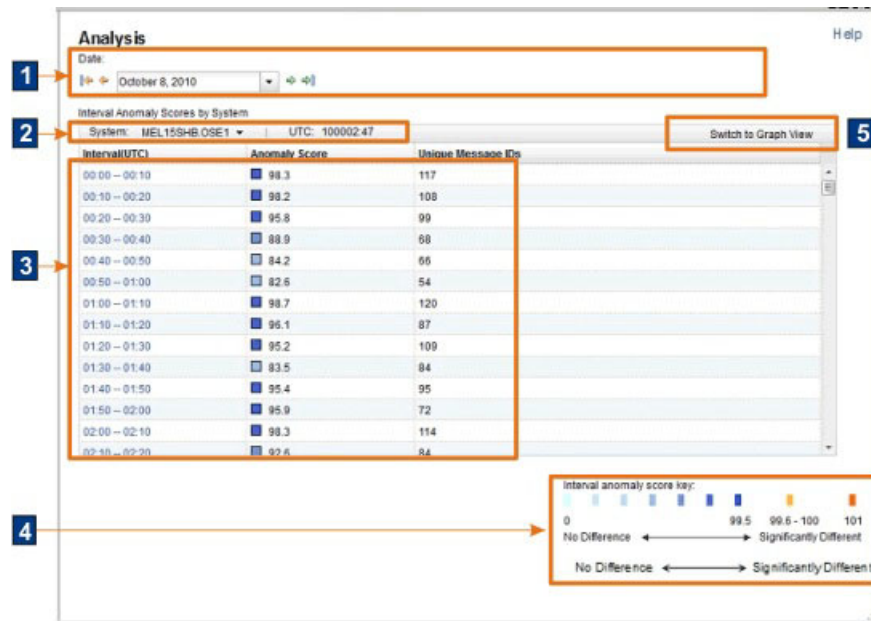


Figure 34. A sample **Analysis** page in tabular format

The tabular view of the **Analysis** page contains the following controls and analytical data.

- The **Date** field displays the currently selected date. You can change the current day to any prior date for which IBM zAware has analytic data. You can type the date or select it from the calendar widget.
- The **Interval Anomaly Scores by System** table contains a toolbar through which you can alter the display.
 - Through the **System** list, you can select a different system for which you want to display analytical data. In this list, each monitored client is identified by sysplex and system name, in the format `sysplex_name.system_name`; for example: `SYSPLEX1.SYSA`. This list contains the names of all systems that are currently or have been previously connected to IBM zAware. By default, the first system displayed is the first viewable system in the graphical view of the Analysis page.
 - For the selected system displayed in the System list, IBM zAware provides the UTC offset for the time zone in which the selected system resides.
 - Through **Switch to Graph View**, you can return to the default graphical format of the **Analysis** page.
- The **Interval Anomaly Scores by System Table** contains the following analytical data for the selected system.
 - The **Interval (UTC)** column contains the start and end of each 10-minute interval for the selected date, in Coordinated Universal Time (UTC), using the 24-hour clock. To access detailed message information, click an interval in the Interval (UTC) column to open the Interval view.
 - The **Anomaly Score** column contains one colored square for each 10-minute interval, along with the anomaly score for this interval. The server builds this analytical data by comparing current data from the client to the model for that client. The analytical data in the **Anomaly Score** column is refreshed automatically, every two minutes.

- The **Unique Message IDs** column contains the number of unique message identifiers (IDs) that were issued within the 10-minute interval.

4. The **Interval anomaly score key** correlates the color of an interval in the bar graph to its relative anomaly score. The interval anomaly score indicates unusual patterns of message IDs within a given interval, as compared to the model of normal system behavior for a specific system.

The interval anomaly scores range from 0 to 101. A score of 0 means that the IBM zAware server detected no difference from the system model for the interval; the interval contains expected messages and message clusters that match the model. A score of 101 means that the server detected significant differences from the system model; the interval contains one or more new messages or many messages issued out of context. The server also assigns a score of 101 for the following conditions:

- The interval contains one or more messages that IBM rules define as a critical message.
- The interval receives an anomaly score that is greater than twice the largest interval score in the model.

Intervals with lower scores are colored with varying shades of blue. Intervals with higher scores are colored with the darkest shade of blue, or with gold or orange.

The interval anomaly scores are:

0 through 99.4

The interval contains messages and message clusters that match or exhibit relatively insignificant differences in expected behavior, as defined in the IBM zAware model. A score of 0 is possible because the server eliminates all expected, in-context messages from its scoring calculation. A score of 0 indicates intervals that exhibit no difference in behavior compared to the system model. In the bar graph display, these intervals are colored with the lightest blue shade.

Intervals with scores that are greater than 0 but less than 99.5 contain some messages that are unexpected or issued out of context. Scores in this range indicate intervals that do not vary significantly from the system model. In the bar graph display, these intervals are colored with varying shades of blue.

99.5 Intervals with this score contain some rarely seen, unexpected, or out-of-context messages. Generally speaking, this score indicates intervals with some differences from the system model but do not contain messages of much diagnostic value. In the bar graph display, these intervals are colored with the darkest blue shade.

99.6 - 100

Intervals with this score contain rarely seen messages (these messages appear in the model only once or twice), or many messages that are unexpected or issued out of context. This score indicates intervals with more differences from the system model; these intervals can contain messages that might help you diagnose anomalous system behavior. In the bar graph display, these intervals are the color gold.

101 Intervals with this score exhibit the most significant differences from the system model; these intervals contain messages that merit investigation. In the bar graph display, these intervals are the color orange. IBM zAware assigns this score to intervals that contain:

- Unique message IDs that the server has not detected previously in the client model
- Unusual or unexpected messages
- Messages that IBM rules define as critical
- A much higher volume of messages than expected

Using the Interval view to pinpoint the causes of system anomalies

You can use the Interval view to diagnose the problem that is causing a particular IBM zAware monitored system to behave abnormally during a specific 10-minute time interval. While the Analysis page provides a clear visual indication of systems that are experiencing anomalous behavior, the Interval view helps you pinpoint and diagnose the causes of this behavior.

Through the diagnostic details in the **Interval view** display, you can answer these questions:

- What message IDs are unusual?
- How often did the unusual message get issued?
- Are messages issued in context within an expected pattern?
- Is a specific z/OS component or application issuing unusual messages?
- Within the 10-minute interval, when did the message ID first appear?

To display the Interval view, click the bar for any of the 10-minute time intervals that are shown in the bar graph on the Analysis page. The controls and content displayed in the Interval view are described in the following sections:

- “Interval view controls and content”
- “Tips for using the Interval view” on page 123

To return to the Analysis page, click **Return to Analysis**.

Interval view controls and content

Figure 35 shows a sample **Interval view**. To display the **Interval view**, click the colored rectangle for any one of the 10-minute time intervals in the bar graph of the **Analysis** page.

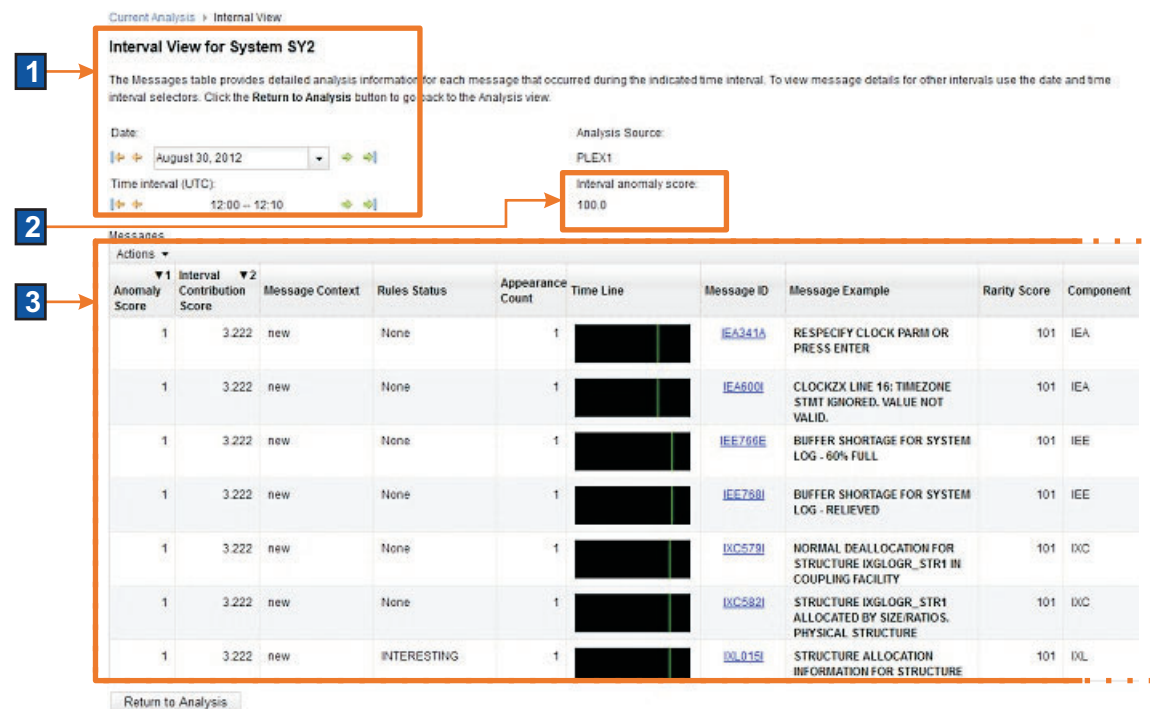


Figure 35. A sample **Interval view** display

The **Interval view** display contains the following controls and diagnostic details:

1. The system name, the date, and the time interval that you selected from the **Analysis** page.

Date The **Date** field displays the currently selected Coordinated Universal Time (UTC) date. You can change the current day to another date.

Time interval

The **Time interval** field displays the start and end times for the selected 10-minute interval in UTC, using the 24-hour clock. To change the selected interval, use the increment (↗) and decrement (↘) arrows to scroll by 10-minute interval, and use the large increment (↗) and large decrement (↘) arrows to scroll by hour.

2. The **Interval anomaly score**, which indicates the relative difference in behavior, as compared to the system model.

The interval anomaly scores range from 0 to 101. A score of 0 means that the IBM zAware server detected no difference from the system model for the interval; the interval contains expected messages and message clusters that match the model. A score of 101 means that the server detected significant differences from the system model; the interval contains one or more new messages or many messages issued out of context. The server also assigns a score of 101 for the following conditions:

- The interval contains one or more messages that IBM rules define as a critical message.
- The interval receives an anomaly score that is greater than twice the largest interval score in the model.

Intervals with lower scores are colored with varying shades of blue. Intervals with higher scores are colored with the darkest shade of blue, or with gold or orange.

3. The **messages table**, which contains details about every unique message ID issued during the interval. If the same message ID was issued more than once during the selected interval, the message table contains only one entry for that unique message ID. The details displayed for each message include:

Anomaly Score

Indicates the difference in expected behavior for this specific message ID within the selected interval. The message anomaly score is a combination of the interval contribution score for this message and the rule, if any, that is in effect for this message. Higher scores indicate greater anomaly so messages with high anomaly scores are more likely to indicate a problem. The message anomaly score ranges from 0 through 1.0.

Interval Contribution Score

Indicates the relative contribution of this message to the anomaly score for the 10-minute interval. This interval score is a function of the rarity score, the number of times that the message appears within this interval, and whether the message appeared in context. Higher scores indicate greater contribution to the interval anomaly score. The interval contribution score ranges from 0 through the largest number that the Java double data type supports.

Message Context

Indicates whether or not this message is part of an expected pattern of messages associated with a routine system event (for example, starting a subsystem or workload). IBM zAware identifies and recognizes these patterns or groups, which are called “clusters”, and the specific message IDs that constitute a specific cluster. When analyzing data from a monitored client, the server determines whether a specific message is expected to be issued within a specific cluster. A message that is issued out of context (without the other messages in the same cluster) might indicate a problem.

Values for Message Context are:

New IBM zAware has not previously detected this message in the client model.

Unclustered

This message is not part of a defined cluster.

In context

This message was issued as expected, within a cluster to which this message belongs.

Out of context

This message is expected to be issued as part of a specific cluster but was issued in a different context.

Rules Status

Indicates whether or not the IBM zAware server applied a rule to determine the message anomaly score. The rule can be one of the following:

- Predefined by IBM.
- Assigned by IBM zAware as a result of the analysis of training data.
- Assigned by IBM zAware when an administrator has identified the message as one that IBM zAware is to ignore during analysis, either until the next model is built or until an administrator manually resets the ignore status.

An administrator cannot identify a message to be ignored when an IBM rule already applies to that message. An IBM rule takes precedence, even when an administrator has already successfully marked the message to be ignored. This situation can occur when an administrator has successfully designated a message to be ignored, but IBM zAware later assigns an IBM rule to that message, as a result of the analysis of training data. In this case, the IBM rule is displayed in this column.

Possible values for this field are:

Critical

An IBM rule identifies this message as critical for diagnosing a potential system problem. For example, message IXC101I, which indicates that a system is being removed from a sysplex, is classified as critical.

Important

An IBM rule identifies this message as likely to indicate a problem. For example, message IEA911E, which indicates that an SVC dump has been taken, is classified as important.

Interesting

An IBM rule identifies this message as indicative of a diagnostically useful event, such as a health check exception.

None No rule is applied for this message.

Non-Interesting

A predefined IBM rule or an IBM zAware-assigned rule identifies this message as one with little or no diagnostic value.

User Ignored

An administrator has identified the message as one that IBM zAware is to ignore during analysis, either until the next model is built or until an administrator manually resets the ignore status.


For only those users with an ID mapped to the Administrator role, an icon () is displayed in the column to indicate whether the rules status can be modified. Click the icon to open the Ignore Message Status window to view the current ignore status for this message ID.

Figure 36 shows a sample view of the Ignore Message Status window.

Ignore Message Status

The current ignore status for the selected message ID is shown in the following information. To change this status for future intervals on the current system, select a different ignore message option in the list and click OK.

| | |
|------------------------|--------------------------------------|
| Selected message ID: | Current system: |
| JVMDMP025I | UTCPLXCB.CB8E |
| Current ignore status: | Current ignore status applied (UTC): |
| Not Ignored | N/A |

Ignore message option for future intervals:

☒ Do not ignore message. (current status)

☐ Ignore message until next training occurs for the current system.

☐ Ignore message until manually restored. Messages can be restored using the Manage Ignored Messages action in the Training Sets task.

☐ Go to Manage Ignored Messages view on OK.

Figure 36. The Ignore Message Status window

For a description of the Ignore Message Status window, see “Ignore Message Status window” on page 126.

“Managing ignored messages” on page 164 provides more information about assigning an ignore status to specific messages.

Appearance Count

Specifies the number of times that this message was issued within the selected 10-minute interval.

Time Line

Provides an illustration of when this message was issued within the selected 10-minute interval. Each line represents one minute during the interval in which the message was issued. To display the text-only format, position your cursor over the graphic display in the Time Line column on the Interval View, and click to open the Time Line Summary window.

Figure 37 shows a sample tabular view of the Time Line column contents.

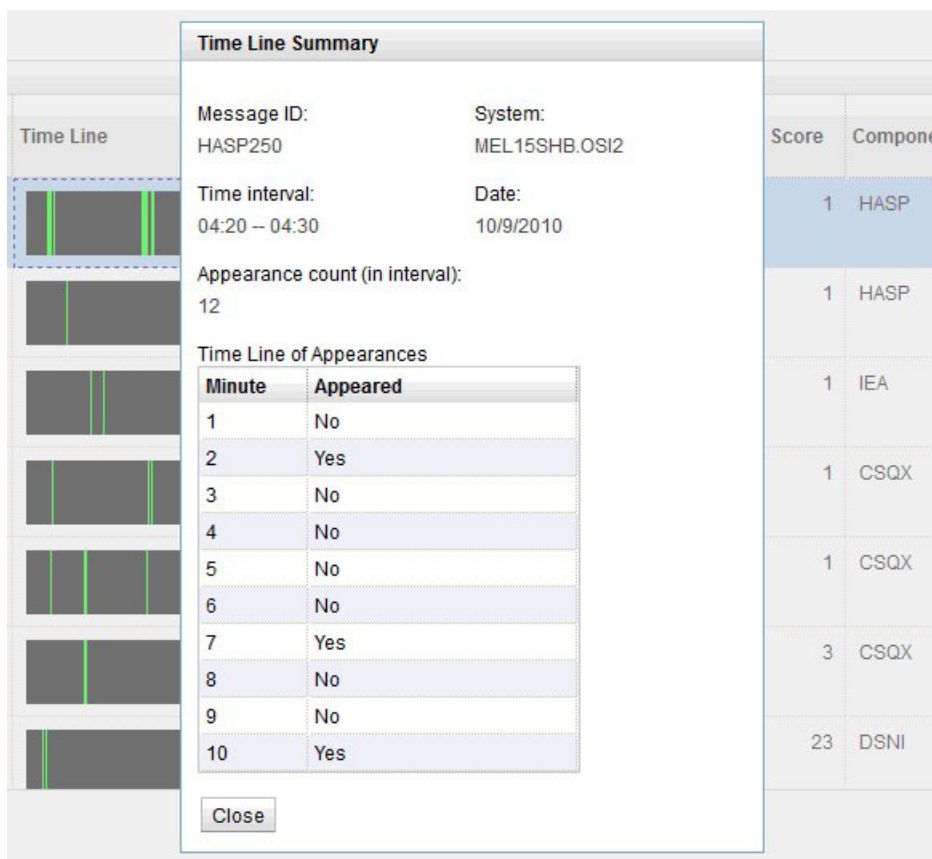


Figure 37. The Interval view Time Line in tabular (text-only) format

For a description of this text-only view, see “Time Line Summary window” on page 125.

Message ID

Provides the message identifier. The message ID itself is a link through which you can open a browser window, and search for an online description by using the Internet search engine of your choice.

Message Example or Message Summarization

Provides either the full message text for the first occurrence of this message within the interval, or a summary of the common message text that was issued for each occurrence of

the same message. For summaries, only common text is displayed, with asterisks replacing any text that differs between occurrences of this message.

By default, this column displays the full message text with the column heading **Message Example**. To change the display to the summary view, click **Actions > View Message Summary**. To reset the display to the default example view, click **Actions > View Message Full Text**.

Rarity Score

Indicates how often this message was issued within the collection of 10-minute intervals used to build the model of system behavior. Values range from 1 to 101:

- A value of 1 indicates that the message is issued in almost all intervals in the model.
- A value of 100 indicates that the message is issued in almost none of the intervals in the model.
- A value of 101 indicates that this message ID has not been issued in any interval in the model.

Component

Identifies the system component or application that issued this message. For z/OS, the identifiers are 3- or 4-character IDs that represent components listed in *z/OS MVS Diagnosis: Reference*, GA22-7588.

Cluster ID

Provides the identifier of the cluster to which this message belongs. When the message is not part of a recognized cluster, the cluster ID is -1.

Tips for using the Interval view

To find those messages in the **Interval view** that have the most value for diagnosis, use the following tips:

- The message anomaly score is the primary indicator of diagnostic value, so the default organization of the Message table in the **Interval view** arranges message entries sorted first by **Anomaly Score** in descending order, from highest value to lowest, and then by **Interval Contribution Score** in descending order, from highest value to lowest.

Sorting by **Interval Contribution Score**, in descending order, moves messages of little or no diagnostic value to the bottom of the Messages table. Given that the Messages table contains one entry for each unique message issued during the selected interval, this sorting helps you avoid scrolling through a considerable number of insignificant message entries.

- To reorganize the default presentation of the Message table for the current Interval view:
 - Click **Actions > View Message Summary** or **ActionsView Message Full Text** to display either the Message Example or Message Summarization column.

By default, this column displays the full message text with the column heading **Message Example**. To change the display to the summary view, click **Actions > View Message Summary**. To reset the display to the default example view, click **Actions > View Message Full Text**.
 - Click a single column heading to resort the message entries according to the values in that specific column.
 - Click **Actions > Sort Multiple** to rearrange the display by selecting up to three columns to sort. The IBM zAware GUI presents the Select Nested Sort Attributes window, through which you can make selections to hierarchically sort up to three columns.

When you click OK on the Select Nested Sort Attributes window, the column headings in the resulting **Interval view** display contain numbers to identify the priority of the columns that you selected, as well as symbols to indicate whether you selected ascending or descending sort order of the column contents.

| Actions ▼ | | | | | | | |
|---------------|--------------------|-----------------|--------------|------------------|-----------|------------|-----------------|
| ▼1 | Interval | ▼2 | | | ▼3 | | |
| Anomaly Score | Contribution Score | Message Context | Rules Status | Appearance Count | Time Line | Message ID | Message Example |

For a description of the Select Nested Sort Attributes window, see “Select Nested Sort Attributes window.”

Any changes that you make to the Interval view apply only for the current display. If you return to the Analysis page and then select an interval to open another Interval view, IBM zAware uses the default presentation for the Messages table.

- If several of the messages with the highest anomaly scores and interval contribution scores were issued by the same system component or application, consider sorting by **Component** to view all messages issued by a particular component.

Select Nested Sort Attributes window

You can use the Select Nested Sort Attributes window to sort a table based on the values in up to three columns.

To display the Select Nested Sort Attributes window, select **Sort Multiple** from the **Actions** list provided in the Messages table on the Interval view.

Tip: When you use the Select Nested Sort Attributes window to specify your sort criteria, you are required to specify a sort for at least two columns. To sort on the values in a single column only, click the column header in the Messages table.

Fields in the Select Nested Sort Attributes window

Table 25 lists and describes the fields included in the Select Nested Sort Attributes window.

Table 25. Fields in the Select Nested Sort Attributes window

| Field | Description |
|-------------|---|
| First sort | Name of the column you want sorted first and the direction (ascending or descending) in which you want it to be sorted. A first sort is required. |
| Second sort | Name of the column you want sorted second and the direction (ascending or descending) in which you want it to be sorted. A second sort is required. |

Table 25. Fields in the Select Nested Sort Attributes window (continued)

| Field | Description |
|------------|---|
| Third sort | Name of the column you want sorted third and the direction (ascending or descending) in which you want it to be sorted. Sorting on a third column is optional. If you opt not to have a third sort, select Do Not Sort . |

Sorting process

When the table is sorted, the following process is used:

1. The values in the column identified as the *first sort* are sorted first in the direction specified.
2. The values in the column identified as the *second sort* are sorted within the first sort in the direction specified.
3. The values in the column identified as the *third sort* are sorted within the first and second sorts in the direction specified.

The arrangement of the values depends on the code page of your Web browser, which might use character casing (upper or lower) as a factor for sorting.

IBM zAware displays arrows in the column header to indicate whether the sort is ascending (▲) or descending (▼). If two or more columns are sorted, the number 1 (first sort), 2 (second sort), or 3 (third sort) is displayed next to the arrow to indicate the order of the sort.

Time Line Summary window

The Time Line Summary window provides a text-only format that indicates when a selected message ID was issued during a selected 10-minute interval.

To display the text-only format, position your cursor over the graphic display in the Time Line column on the Interval View, and click to open the Time Line Summary window.


Fields in the Time Line Summary window

Table 26 describes the fields that are displayed in the Time Line Summary window.

Table 26. Fields displayed in the Time Line Summary window

| Fields | Description |
|--------------------------------|--|
| Message ID | Identifies the message ID selected from the Messages table in the Interval view. |
| System | Identifies the name of the system on which the selected message ID was issued. |
| Time interval | Specifies the time range (in Coordinated Universal Time, using the 24-hour clock) for the selected 10-minute interval. |
| Date | Specifies the date on which the selected 10-minute interval occurred. |
| Appearance count (in interval) | Specifies the total number of times that the selected message ID was issued during the selected 10-minute interval. |
| Time Line of Appearances | Specifies whether or not the selected message ID was issued during each minute of the selected 10-minute interval. |
| Close | Closes the Time Line Summary window and returns to the Interval view. |

Ignore Message Status window

You can use the Ignore Message Status window to display the current status for a specific message ID. To display the Ignore Message Status window, click the icon () in the Rules Status column in the Interval view. Only those users with an ID mapped to the Administrator role can view the icon and click it to open the Ignore Message Status window.

Fields in the Ignore Message Status window

Table 27 describes the fields that are displayed in the Ignore Message Status window.

Table 27. Fields displayed in the Ignore Message Status window

| Field | Description |
|--|---|
| Selected message ID | Lists the message ID selected from the Messages table in the Interval view. |
| Current system | Lists the name of the system on which the selected message ID was issued. |
| Current ignore status | <p>Lists the current ignore status. Possible values are:</p> <p>Not Ignored The message ID does not have any ignore status value currently applied to it.</p> <p>Until next training The message is to be ignored during analysis until the next time IBM zAware successfully builds a model of behavior for the monitored system, as the result of either a manually requested or automatically scheduled training operation. The date and time for the next scheduled model rebuild is listed under “Next scheduled training date” after you select Next Training Period Model Dates on the Manage Model Dates page.</p> <p>Until manually restored The message is to be ignored during analysis until an administrator manually changes the ignore status of the message, or removes it from the list of messages in the Ignored Messages table.</p> |
| Current ignore status applied (UTC) | Indicates the date and time (in UTC, using the 12-hour clock) at which an administrator most recently updated the ignore status for the message. |
| Ignore message option for future intervals | <p>Lists the options for setting ignore status for this message ID. By default, the current status is selected.</p> <p>You can select one of the following options.</p> <ul style="list-style-type: none">• Do not ignore message.• Ignore message until next training occurs for the current system.• Ignore message until manually restored. Messages can be restored using the Manage Ignored Messages action on the Training Sets page. |
| OK | Sets the selected ignore message option and closes the Ignore Message Status window. If you want to go to the Manage Ignored Messages page instead of returning to the Interval view, click Go to Manage Ignored Messages view on OK . For information about the Manage Ignored Messages page, see “Managing ignored messages” on page 164. |
| Cancel | Closes the Ignore Message Status window and returns to the Interval view. |

Table 27. Fields displayed in the Ignore Message Status window (continued)

| Field | Description |
|---|--|
| Go to “Manage Ignored Messages” view on OK. | Opens the Manage Ignored Messages page. For information about the Manage Ignored Messages page, see “Managing ignored messages” on page 164. |

Verifying planned system changes with IBM zAware

Although the **Analysis** page display is useful for finding and diagnosing unexpected problems or reported incidents, you also can use it to verify behavior after a planned change. If you know when your installation made a change, you can navigate to the time period immediately following that change and view the analytical data for the affected monitored client (system). For example, you can check the intervals roughly one hour after a system IPL to verify that the system is operating normally.

A higher volume of messages might indicate a potential problem after the following types of changes:

- Software updates for the operating system, middleware, or applications
- Updated system settings
- Changed system configurations, including hardware

Software updates and configuration changes might not result in higher interval anomaly scores for the affected system. When your installation introduces new workloads or applications to a system, however, IBM zAware scores the intervals that follow these changes as highly anomalous because it detects messages that are not reflected in the system model. IBM zAware is not able to detect whether these new messages indicate problems or routine, expected behavior until enough data is available to update the system model.

After using the IBM zAware analytical data to verify that the new workload or application is operating as expected, you have two options for altering IBM zAware analysis to prevent the assignment of high anomaly scores to future intervals: Marking messages for IBM zAware to ignore during analysis, or manually requesting IBM zAware to rebuild the model of system behavior.

Marking messages for IBM zAware to ignore

You can mark messages from the new workload or application for IBM zAware to ignore during analysis. You can designate messages to be ignored until the next time IBM zAware builds a model of behavior for the monitored system, or until an administrator manually changes the ignore status of the message.

Ignore messages until next training occurs for the current system.

Marks the selected messages to be ignored during analysis until the next time IBM zAware successfully builds a model of behavior for the monitored system, as the result of either a manually requested or automatically scheduled training operation. The date and time for the next scheduled model rebuild is listed under “Next scheduled training date” after you select **Next Training Period Model Dates** on the Manage Model Dates page.

Use this value for messages that you have determined to be anomalous because of a workload change on the system, but you expect them to become part of the normal behavior for this system. The next training results in a model that includes these messages, which will be subject to normal analysis after the training.

Ignore messages until manually restored.

Marks the selected messages to be ignored during analysis until an administrator manually changes the ignore status of the message, or removes it from the list of messages in the Ignored Messages table.

Use this value for messages that you have determined to be normal (that is, not indicative of a problem) on this system. In subsequent analysis, these messages do not contribute to the anomaly score, and thus reduce false-positive results.

This option is the most expedient method; however, if you choose to ignore messages until the next training, note that IBM zAware includes the designated messages in analysis immediately after the successful completion of either a manually requested or automatically scheduled training operation. For more information about designating messages to be ignored during analysis, see “Managing ignored messages” on page 164.

Manually requesting IBM zAware to rebuild a model

You can manually request IBM zAware to rebuild the model of system behavior.

This option requires specific timing to be effective. The sequence of events shown in Figure 38 illustrates how you can use this option to alter IBM zAware analysis after installing a new application on a system named SYS1.

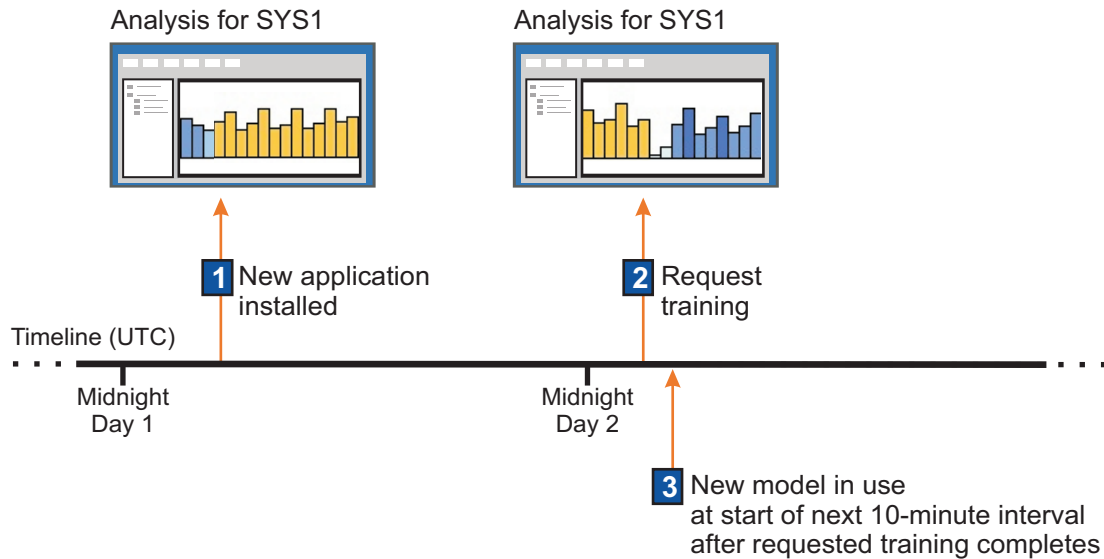


Figure 38. Sample timeline for retraining IBM zAware to analyze data from a new application

1. Several hours after midnight on Day 1, your installation installs a new application on SYS1, which is connected and sending data to the IBM zAware server.
Before the installation occurred, the analytical data in the **Analysis** page indicates fairly normal system behavior with blue rectangles. After the installation, intervals in the **Analysis** page are dark gold because the server detects unique messages that it has not detected previously in the model for SYS1. The server assigns an interval anomaly score of 101 to each interval in which the new application issues a message.
2. Although you can request the server to rebuild a model at any time, wait until midnight of Day 2 before you request the IBM zAware server to rebuild the model for SYS1.
This delay is necessary because the server uses only complete days of data to build models, and because it needs a significant amount of data from the new application to correctly identify and recognize message patterns. Any time after midnight on Day 2, you can request the server to rebuild the SYS1 model by using the **Request Training** action on the **Administration > Training Sets** page. The server uses the data it received from SYS1 during Day 1 to update the model.
3. After the requested training completes, the IBM zAware server begins to use the newly rebuilt model at the start of the next 10-minute interval.
Using the new model, the server can more accurately detect message patterns from the new application, and intervals receive more accurate interval anomaly scores and colors. The effect of retraining depends on the stability of the system and the degree to which the new messages cluster together, so you might need to wait another day to collect additional data and rebuild the model again.

Chapter 15. Specifying security settings for the IBM zAware GUI

To access the IBM zAware graphical user interface (GUI), a user requires a valid user ID and password to authenticate with the IBM zAware GUI and users must be assigned to an IBM zAware role, which permits access to IBM zAware functions.

IBM zAware supports two methods of user authentication. You can authenticate users through the use of a Lightweight Directory Access Protocol (LDAP) repository or through the use of a local file-based repository. For simplicity, using an LDAP repository only is the preferred option. However, you might want to define one or two user IDs in a local repository so you can access the IBM zAware GUI when the LDAP server is unavailable. If you configure an LDAP repository and also define users or groups in a local repository, both sets of users or groups are available through the IBM zAware GUI. Do **not** define the same user ID in more than one repository; results are unpredictable.

With either type of repository, the authentication process is the same:

1. A user enters a user ID and password to log in to the IBM zAware GUI.
2. The IBM zAware server verifies that the login credentials match a user ID and password stored in the LDAP repository or the local repository.
3. If there is a match, the user is considered to be authenticated. However, IBM zAware does not grant the user access to the GUI until it verifies that a user is also assigned to an IBM zAware role – *User* or *Administrator*.

When your installation configures and activates the IBM zAware partition, your installation defines a master user ID and password that you can use to initially log in to the IBM zAware GUI. By default, the master user ID is assigned to the administrator role, which has authority to perform any task that is available through the IBM zAware GUI.

To configure your security settings for the first time, log in to the GUI using the master user ID and password. IBM zAware provides the following security mechanisms that your installation can configure to limit access to the IBM zAware GUI:

Server SSL certificate

You can, optionally, replace the automatically generated Secure Sockets Layer (SSL) certificate that is configured in the IBM zAware server with a certificate that is signed by a certificate authority. Doing so prevents the browser warning message that is displayed when you initially log in to the IBM zAware GUI. For instructions, see “Replacing the default SSL certificate” on page 130.

LDAP authentication for the IBM zAware GUI

You can, optionally, configure the IBM zAware server to authenticate users through the use of an existing LDAP repository. For instructions, see “Enabling LDAP authentication for IBM zAware users” on page 133.

For instructions for using the local file-based repository for authentication, see Chapter 20, “Setting up a local repository to secure access to the IBM zAware GUI,” on page 185.

Role-based access to IBM zAware GUI functions

You can control access to IBM zAware GUI functions by assigning users to specific IBM zAware roles. For instructions, see “Assigning users or groups to a role” on page 137.

Browser session timeout setting

You can change the browser session time out from the default setting to a value that is more appropriate for your installation. By default, browser sessions time out after 12 hours (720 minutes). For instructions, see “Specifying the duration of a browser session” on page 141.

These security mechanisms are described in more detail in the sections that follow.

Replacing the default SSL certificate

A Secure Sockets Layer (SSL) certificate is automatically generated for IBM zAware when your installation performs the initial activation of the IBM zAware partition. This certificate is not signed by a certificate authority (CA); therefore, the first time you log in to the IBM zAware graphical user interface (GUI), the browser displays a warning message because it does not recognize the default SSL certificate. You can resolve this problem by replacing the default SSL certificate with a certificate signed by a certificate authority of your choice. Doing so provides secure communication between the IBM zAware server and the browsers of all authorized users.

Before you begin

If you decide to replace the automatically generated certificate, which is the recommended practice for improved security, you can use any third-party certificate authority of your choice, or your installation can provide an internal certificate authority for certificate signing tasks. IBM zAware does not renew these replacement certificates; in this case, managing replacement certificates becomes the responsibility of the security administrator.

The Open Directory Project maintains a list of third-party certificate authorities at the following URL.

http://www.dmoz.org/Computers/Security/Public_Key_Infrastructure/PKIX/Tools_and_Services/Third_Party_Certificate_Authorities/

You might need to process the CA reply before you can paste it into the appropriate field in the IBM zAware GUI.

- The required format for replacement certificates is Base64 encoded X509 certificate blocks.
- When you receive a reply from a certificate authority, the reply might contain a chain of certificates, starting with the signed server certificate, possibly followed by certificates from one or more intermediate CAs and, finally, the self-signed certificate of the CA. When you supply this information in the GUI, provide the entire certificate chain, starting with the signed server certificate through the self-signed certificate of the CA.
- In some cases, the CA reply that you receive is delivered in a public-key cryptography standards (PKCS) #7 file. You must extract the certificates from the file before pasting them into the GUI. One method of extracting certificates from a PKCS #7 file is to use the **openssl pkcs7** command; for more information, see the OpenSSL Project web site at the following URL.

<http://www.openssl.org/>

About this task

This security task is optional.

The following procedure might take several days to complete, depending on the time that the certificate authority requires to receive and process your request, and to send a reply. You can complete other tasks in the IBM zAware GUI while you wait for a reply from the certificate authority.

Procedure

1. Expand the Administration category in the navigation pane and select **Configuration**. The Configure Settings page is displayed.
2. Click **Security > SSL Settings** to display the SSL Settings tab.
3. To create a certificate signing request (CSR), in the Certificate Actions section, click **Generate Certificate Signing Request**. The Create Certificate Signing Request page is displayed.
4. Enter the appropriate information for the following fields:

- a. In the **Common name** field, verify the host name or IP address of the IBM zAware partition. IBM zAware preloads this field with a value that matches the host name or IP address specified on the **zAware** page in the image profile of the IBM zAware partition. The host name is required.
 - b. In the **Organization** field, enter the name of your company. The value that you supply for this field must be a string of length 1-64. The organization name is optional.
 - c. In the **Organizational unit** field, enter the company organization or department name. The value that you supply for this field must be a string of length 1-64. The organizational unit is optional.
 - d. In the **Locality** field, enter the city in which your company is located. The value that you supply for this field must be a string of length 1-128. The city is optional.
 - e. In the **State or province** field, enter the state or province in which your company is located. The value that you supply for this field must be a string of length 1-128. The state or province is optional.
 - f. In the **Postal code** field, enter the postal code for your company address. The value that you supply for this field must be a string of length 1-16. The postal code is optional.
 - g. In the **Country code** field, enter the two-character abbreviation for the country in which your company is located. The value that you supply for this field must be a string of length 1-2. The country code is optional.
5. Click **Generate** to generate the certificate request. IBM zAware displays the generated request.
 6. Expand the Generated Request Input section to display and verify the generated request input.
 7. Copy the generated certificate signing request, which is displayed in the **Generated CSR** field.
 8. Submit the request to a certificate authority using the procedures required by that entity.
 9. Click **Close** to return to the main SSL Settings tab.
 10. When you receive a reply from the certificate authority, do the following:
 - a. Extract the certificates, if necessary.
 When you receive a reply from a certificate authority, the reply might contain a chain of certificates, starting with the signed server certificate, possibly followed by certificates from one or more intermediate CAs and, finally, the self-signed certificate of the CA. When you supply this information in the GUI, provide the entire certificate chain, starting with the signed server certificate through the self-signed certificate of the CA.
 Make sure that you do not insert any lines or spaces between the end of one certificate and the beginning of the next certificate. When you paste certificate replies in the GUI, make sure that you include all of the content, including the header -----BEGIN CERTIFICATE----- through and including -----END CERTIFICATE-----
 If you need to view a sample CA reply that contains a certificate chain, see Appendix B, "Sample certificate authority (CA) reply," on page 209.
 - b. Return to the main SSL Settings tab.
 - c. Click **Receive Certificate Request Reply**. The Receive Certificate Authority Reply page is displayed.
 - d. Copy the reply to your clipboard and paste it into the **Certificate Authority reply** field.
 - e. Click **Receive** to import the CA reply into the IBM zAware server.

Results

The main SSL Settings tab now displays information from the received CA reply.

SSL Settings tab

Use the actions provided on the SSL Settings tab to replace the default IBM zAware SSL certificate with a certificate that is signed by a certificate authority.

For instructions, see "Replacing the default SSL certificate" on page 130.

For a description of the content and controls included on the SSL Settings tab, see Table 28.

Table 28. Items displayed on the SSL Settings tab

| Item | Description |
|-----------------------------------|---|
| Current zAware Server Certificate | Displays information about the SSL certificate that is configured in the IBM zAware server. |
| Certificate Actions | <p>Provides the following buttons:</p> <p>Generate Certificate Signing Request Allows you to specify the information required to generate a new certificate signing request (CSR) and to generate the request.</p> <p>View Last Generated Request Allows you to view the last certificate signing request that IBM zAware generated. This button is enabled after you generate the CSR.</p> <p>Receive Certificate Request Reply Allows you to input the reply you received from the certificate authority and to receive that certificate into IBM zAware. This button is enabled after you generate the CSR.</p> |

Create Certificate Signing Request page

Use the Create Certificate Signing Request (CSR) page to specify the information to include in the certificate signing request.

To display the Create Certificate Signing Request page, click **Generate Certificate Signing Request** on the main SSL Settings tab. The fields initially included on the page are described in Table 29.

After you provide the appropriate information, click **Generate** to generate the request. The fields that are included on the page after the CSR is generated are described in Table 30 on page 133.

Table 29. Fields displayed on the page before the CSR is generated

| Field | Description |
|---------------------|---|
| Common name | Verify the host name or IP address of the IBM zAware partition. IBM zAware preloads this field with a value that matches the host name or IP address specified on the zAware page in the image profile of the IBM zAware partition. The host name is required. |
| Organization | Enter the name of your company. The value that you supply for this field must be a string of length 1-64. The organization name is optional. |
| Organizational unit | Enter the company organization or department name. The value that you supply for this field must be a string of length 1-64. The organizational unit is optional. |
| Locality | Enter the city in which your company is located. The value that you supply for this field must be a string of length 1-128. The city is optional. |
| State or province | Enter the state or province in which your company is located. The value that you supply for this field must be a string of length 1-128. The state or province is optional. |
| Postal code | Enter the postal code for your company address. The value that you supply for this field must be a string of length 1-16. The postal code is optional. |
| Country code | Enter the two-character abbreviation for the country in which your company is located. The value that you supply for this field must be a string of length 1-2. The country code is optional. |

Table 30. Fields displayed on the page after the CSR is generated

| Field | Description |
|-------------------------|---|
| Generated Request Input | Provides the input you supplied for the request. Verify the request input. If any information is incorrect, you must create a new request. To do so, click Close to return the to main SSL Settings tab. Then, click Generate Certificate Signing Request . |
| Generated CSR | Provides the certificate signing request that IBM zAware generated using your input. Copy the CSR and submit it to a certificate authority. |

View Last Generated Request page

Use the View Last Generated Request page to view the last certificate signing request that IBM zAware generated.

To display the View Last Generated Request page, click **View Last Generated Request** on the main SSL Settings tab. The fields included on the page are described in Table 31.

Table 31. Fields displayed on the View Last Generated Request page

| Field | Description |
|------------------------------|--|
| Last Generated Request Input | Provides the input that was supplied for the request. |
| Last generated CSR | Provides the certificate signing request that IBM zAware generated using the input. If necessary, copy the CSR and submit it to a certificate authority. |

Receive Certificate Authority Reply page

Use the Receive Certificate Authority Reply page to input the reply you received from the certificate authority and to receive that certificate into IBM zAware.

To display the Receive Certificate Authority Reply page, click **Receive Certificate Request Reply** on the main SSL Settings tab.

In the **Certificate Authority reply** field, which is displayed on the page, enter the reply that you received from the certificate authority. Verify that:

- The format of the reply is Base64 encoded X509 certificate blocks.
- The reply contains the entire certificate chain. When you receive a reply from a certificate authority, the reply might contain a chain of certificates, starting with the signed server certificate, possibly followed by certificates from one or more intermediate CAs and, finally, the self-signed certificate of the CA. When you supply this information in the GUI, provide the entire certificate chain, starting with the signed server certificate through the self-signed certificate of the CA.

In some cases, the CA reply that you receive is delivered in a public-key cryptography standards (PKCS) #7 file. You must extract the certificates from the file before pasting them into the GUI. One method of extracting certificates from a PKCS #7 file is to use the **openssl pkcs7** command; for more information, see the OpenSSL Project web site at the following URL.

Click **Receive** to import the certificate into the IBM zAware server.

Enabling LDAP authentication for IBM zAware users

Lightweight Directory Access Protocol (LDAP) is an information directory where users and groups can be defined only once and shared across multiple machines and multiple applications. IBM zAware can authenticate user login requests against an existing LDAP server. To enable LDAP authentication, specify the settings for an existing LDAP server in your installation.

Before you begin

- Obtain the master user ID and password that was provided on the **zAware** page in the image profile for the IBM zAware partition.
- Check with your LDAP administrator or network administrator to ensure that the IBM zAware server can access the LDAP server. IBM zAware cannot save LDAP settings unless it can communicate with the LDAP server when you apply the new or changed settings.
- Check with your LDAP administrator to determine the settings needed to configure your LDAP server. For a description of each setting, see “LDAP Settings tab” on page 135.
- If you are using this procedure to modify an existing LDAP configuration, make sure you verify that all mapped users and groups are still valid and appropriate in the new LDAP configuration. Before making any changes to the LDAP configuration, go to the **Role Mapping** tab and review the lists of currently mapped users and groups for both the **Administrator** and **User** roles.
- If any users or groups are not appropriate for the new LDAP configuration, select them and click **Remove**. If you need more information about using the controls on the **Role Mapping** tab, see “Assigning users or groups to a role” on page 137.

Procedure

1. Log in to the IBM zAware GUI using the master user ID and password that was provided in the image profile for the IBM zAware partition.
2. Expand the Administration category and select **Configuration**. The Configure Settings page is displayed.
3. Click **Security > LDAP Settings** to display the **LDAP Settings** tab.
4. Specify the settings required for the IBM zAware server to communicate with the LDAP server and authenticate users. For a description of the LDAP settings provided, see “LDAP Settings tab” on page 135.
5. Click **Apply** to save the LDAP settings you specified. When you click **Apply**, the GUI displays a confirmation message to indicate that the web server must be restarted for your changes to be applied. This process might take a considerable amount of time to complete. While the server is restarting, other GUI users receive *page not available* errors until the restart process is complete.
6. Click **OK** to confirm that you want to apply your changes, or click **Cancel**.

What to do next

- To verify that IBM zAware is configured to authenticate against the LDAP server, do the following:
 1. Click **Role Mapping** on the **Security** tab.
 2. Assign your user ID to the *User* or *Administrator* role:
 - a. In the **Role** field, select either **Administrator** or **User** as the role to which you want to assign your user ID.
 - b. Specify a search filter to use to find your user ID in the LDAP directory. You can specify an asterisk (*) as a wildcard value at any position in the filter value.
 - c. Select your user ID in the **Available users** list and click **Add** to move your user ID to the **Current mapped users** list.
 - d. Click **Apply** to save your changes to the role mapping.
 3. Try logging in to the IBM zAware GUI with the user ID and password that is specified for you in the LDAP directory.

If IBM zAware logs you in, LDAP user authentication is working correctly.

- If you cannot log in with LDAP user authentication, verify that:
 - Your user ID and password are correct.
 - The IBM zAware server can access the LDAP server.

- The LDAP settings you specified are correct. To do so, log in to the IBM zAware GUI using the master user ID and password provided on the **zAware** page in the image profile for the IBM zAware partition.
- To allow additional users or groups to access IBM zAware, map users or groups in the new LDAP repository to specific IBM zAware roles. For instructions, see “Assigning users or groups to a role” on page 137.

LDAP Settings tab

You can use the **Security > LDAP Settings** tab on the Configure Settings page to authorize users to access the IBM zAware GUI through the use of a Lightweight Directory Access Protocol (LDAP) repository. To do so, specify the appropriate settings on the **LDAP Settings** tab.

Tip: Your installation can opt to use a local file-based repository for user authentication. For instructions, see Chapter 20, “Setting up a local repository to secure access to the IBM zAware GUI,” on page 185.

The LDAP settings are described in the following sections:

- “General LDAP settings”
- “Group LDAP settings” on page 136

For instructions for enabling LDAP authentication, see “Enabling LDAP authentication for IBM zAware users” on page 133.

To save the LDAP settings you specified, click **Apply**. If necessary, click **Restore** to restore the LDAP configuration values that were in effect before you clicked **Apply**.

Note that to apply the settings, the server is automatically restarted. This process might take a considerable amount of time to complete. While the server is restarting, other GUI users receive *page not available* errors until the restart process is complete.

General LDAP settings

Table 32. General LDAP settings

| Setting | Description |
|-------------------------|---|
| LDAP server hostname | Enter the resolvable host name or IP address of the LDAP server to which you want to connect. The host name is required. |
| LDAP server port | Enter the port on which the LDAP server listens for TCP/IP connections. The value can range from 0 - 65535. The port is required. |
| Follow referrals | <p>A referral is an entity that is used to redirect a client request to another LDAP server. A referral contains the names and locations of other objects. It is sent by the server to indicate that the information the client requested can be found at another location, possibly at another server or several servers.</p> <p>Select one of the following options:</p> <p>Follow Indicates that referrals to other LDAP servers will be followed.</p> <p>Ignore Indicates that referrals to other LDAP servers will be ignored. This option is selected by default.</p> <p>A selection is required.</p> |
| Bind distinguished name | Enter the distinguished name used to bind to the LDAP repository. The name must be a string of length 0-512. If no name is specified, the server binds anonymously. The name is optional. |
| Bind password | Enter the password used to bind to the LDAP directory. The password must be a string of length 0-512. The password is optional. |

Table 32. General LDAP settings (continued)

| Setting | Description |
|-------------------------|--|
| Base distinguished name | Enter the distinguished name of a base entry in the repository. The name must be a string of length 1-512. The name is required. |
| Login attribute | Enter the LDAP attribute of a user entity used to login to the IBM zAware GUI. The attribute must uniquely identify a user in the directory. Typical login attributes include <i>uid</i> , <i>mail</i> , <i>primaryuserid</i> , and so on. The value must be a string of length 1-512. The default value is <i>uid</i> . The login attribute is required. |
| User object classes | Enter the object class or classes that are associated with user entities in the LDAP repository. Delimit multiple object classes with semicolons (;). Typical object classes include <i>Person</i> , <i>ePerson</i> , <i>inetOrgPerson</i> , and so on. The value must be a string of length 1-512. At least one user object class is required. |
| User search bases | Specify the base object of the directory (or level of the directory) from which to start a search for user entities in the LDAP repository. The search bases must be subtrees of the base distinguished name. Delimit multiple search bases with semicolons (;). The value must be a string of length 1-512. The user search base is optional. If unspecified, the base distinguished name is used. |
| SSL enabled | Select this option to enable secure socket communication to the LDAP server. If selected, you must supply the SSL certificate in the LDAP server certificate field. By default, SSL is disabled. |
| LDAP server certificate | Enter the Base64 encoded certificate that is required to validate the certificate of the LDAP server. This certificate should be the signer of the server certificate for the LDAP repository. A certificate is required only when SSL is enabled. |

Group LDAP settings

Table 33. Group LDAP settings

| Setting | Description |
|---------------------------------|--|
| User group membership attribute | Enter the LDAP attribute of a user entity that indicates the groups to which an entry belongs. If your LDAP server does not support the group membership attribute, do not specify this attribute. The value must be a string of length 1-512. The user group membership attribute is optional. |
| User group membership scope | Select the scope of the user group membership attribute. You can select one of the following options: Direct Indicates that the attribute contains only immediate members of the group without members of subgroups. This option is selected by default. Nested Indicates that the attribute contains direct members and members nested within subgroups of this group. All Indicates that the attribute contains all direct, nested, and dynamic members. A selection is required if a value is specified in the User group membership attribute field. |
| Group object classes | Enter the object class or classes that are associated with group entities in the LDAP repository. Delimit multiple object classes with semicolons (;). Typical object classes include <i>groupOfNames</i> , <i>groupOfUniqueNames</i> , and so on. The value must be a string of length 1-512. At least one group object class is required. |

Table 33. Group LDAP settings (continued)

| Setting | Description |
|-----------------------------|--|
| Group search bases | Specify the base object of the directory (or level of the directory) from which to start a search for group entities in the LDAP repository. The search bases must be subtrees of the base distinguished name. Delimit multiple search bases with semicolons (;). The value must be a string of length 1-512. The group search base is optional. If unspecified, the base distinguished name is used. |
| Group member attributes | For each group object class specified in the Group object classes field, indicate the LDAP attribute of a group entity in the object class that contains the members of the group. Delimit multiple group member attributes with semicolons (;). A value is required, and must be a string of length 1-512. For example, if the group object classes specification is <i>groupOfNames;groupOfUniqueNames</i> , the group member attributes specification might be <i>member;uniqueMember</i> . |
| Group member object classes | For each attribute specified in the Group member attributes field, specify the object classes of the group that uses the member attribute. The value must be a string of length 1-512. The group member object classes are optional. If unspecified, the member attributes apply to all group object classes. |
| Group member scope | Select the scope of the group member attribute. You can select one of the following options: Direct Indicates that the member attribute contains only direct members. This option is selected by default. Nested Indicates that the member attribute contains both direct and nested members. All Indicates that the member attribute contains direct, nested, and dynamic members. A selection is required. |

Assigning users or groups to a role

In IBM zAware, a role represents the ability to perform one or more tasks in the IBM zAware graphical user interface (GUI). To assign users or groups to an IBM zAware role, use the **Security > Role Mapping** tab on the Configure Settings page.

Before you begin

Configure user authentication for the IBM zAware GUI. You can configure IBM zAware to authenticate users against a Lightweight Directory Access Protocol (LDAP) repository or a local file-based repository.

For more details, see one of the following topics:

- “Enabling LDAP authentication for IBM zAware users” on page 133
- Chapter 20, “Setting up a local repository to secure access to the IBM zAware GUI,” on page 185.

About this task

You can map authorized users and groups to specific roles: either Administrator or User. Users or groups with Administrator authority can use any task in the GUI, while those with User authority can view only the following pages and use only the actions as noted:

- On the graphic or tabular **Analysis** page, all controls and actions are permitted.
- On the **Interval view**, all controls and actions are permitted except for modifying the non-IBM rules status for a specific message ID. Only administrators can view and change a rules status value. IBM rules cannot be changed.

- | • On the **Notifications** page, all actions are disabled.
 - | • On the **System Status** page, all actions are disabled.
- | This procedure describes how to add a user or group to a specific role, and how to remove a user or group from a role.
- | • Only a person with a user ID mapped to the Administrator role can add or remove users or groups from a role.
 - | • An administrator cannot remove his or her user ID from the Administrator role. If an administrator attempts to remove the user or group through which his or her user ID is mapped to the Administrator role, IBM zAware rejects the removal request unless a duplicate Administrator role mapping exists for this administrator's user ID, either through an additional group or an individual user ID mapping.

Procedure

1. Log in to the IBM zAware GUI using the user ID and password that was provided in the hardware definition for the IBM zAware partition.
2. Expand the Administration category in the navigation pane and select **Configuration**. The Configure Settings page is displayed.
3. Click **Security > Role Mapping** to display the **Role Mapping** tab.
4. In the **Role** field, select either **Administrator** or **User** as the role to which you want to map particular users or groups.
The IBM zAware server populates the **Current mapped users** and **Current mapped groups** lists with all users or groups that are currently mapped to the selected role. Initially, only the default master user ID appears in the **Current mapped users** list for both the Administrator role and the User role.
5. Specify the search filter to use when selecting user and group entries from the LDAP directory or local repository. You can specify an asterisk (*) as a wildcard value at any position in the filter value. An asterisk (*) is the default filter value. A filter value is required.
The IBM zAware server populates the **Available users** and **Available groups** lists with user and group entries in the LDAP repository or local repository that match the search filter.
6. Specify the maximum number of matching entries the IBM zAware server can display in the **Available users** and **Available groups** lists. A search limit is required and must be a whole number in the range of 1-200. The default value is 20.
The search limit applies to both users and groups; therefore, a search limit of 20 might return 40 entries: 20 users and 20 groups.
7. To add a user or group to the selected role, complete one or more of the following actions:
 - Select one or more users from the **Available users** list and click **Add** to move the users to the **Current mapped users** list.
 - Click **Add All** to move all the users to the **Current mapped users** list.
 - Select one or more groups from the **Available groups** list and click **Add** to move the groups to the **Current mapped groups** list.
 - Click **Add All** to move all the groups to the **Current mapped groups** list.
8. To remove a user or group from the selected role, complete one or more of the following actions:
 - Select one or more users from the **Current mapped users** list and click **Remove** to move the users to the **Available users** list.
 - Click **Remove All** to move all the users to the **Available users** list.
 - Select one or more groups from the **Current mapped groups** list and click **Remove** to move the groups to the **Available groups** list.
 - Click **Remove All** to move all the groups to the **Available groups** list.
9. Click **Apply** to save your changes to the role mapping. The Apply Role Mappings window is displayed.

10. Review your role assignments. If the changes are correct, click **Apply**.

Results

The IBM zAware GUI displays a confirmation message to indicate that the server must be restarted for the new role mappings to be applied. This process might take a considerable amount of time to complete because the server is automatically restarted with the new role mapping values. While the server is restarting, other GUI users receive *page not available* errors until the restart process is complete.

Role Mapping tab

You can use the **Security > Role Mapping** tab on the Configure Settings page to assign users or groups to an IBM zAware role, which permits them access to function provided in the IBM zAware graphical user interface (GUI).

Important: Before you can map users or groups to roles, you must configure IBM zAware to authenticate users against a Lightweight Directory Access Protocol (LDAP) repository or a local file-based repository. Otherwise, the **Role Mapping** tab displays only the master user ID that was provided in the partition hardware definition.

For more details, see one of the following topics:

- “Enabling LDAP authentication for IBM zAware users” on page 133
- Chapter 20, “Setting up a local repository to secure access to the IBM zAware GUI,” on page 185.

For instructions for assigning users or groups to a role and for a description of what tasks a role authorizes users or groups to perform, see “Assigning users or groups to a role” on page 137.

For a description of the items included on the **Role Mapping** tab, see Table 34.

Table 34. Items displayed in the Role Mapping tab

| Item | Description |
|----------------------|---|
| Role | <p>Indicates the role to which users or groups are or will be assigned. Select User or Administrator. A selection is required.</p> <p>The IBM zAware server populates the Current mapped users and Current mapped groups lists with all users or groups that are currently mapped to the selected role. Initially, only the default master user ID appears in the Current mapped users list for both the Administrator role and the User role.</p> |
| Filter | <p>Specify the search filter to use when selecting user and group entries from the LDAP directory or local repository. You can specify an asterisk (*) as a wildcard value at any position in the filter value. An asterisk (*) is the default filter value. A filter value is required.</p> <p>The IBM zAware server populates the Available users and Available groups lists with user and group entries in the LDAP repository or local repository that match the search filter.</p> |
| Search limit | <p>Specify the maximum number of matching entries the IBM zAware server can display in the Available users and Available groups lists. A search limit is required and must be a whole number in the range of 1-200. The default value is 20.</p> <p>The search limit applies to both users and groups; therefore, a search limit of 20 might return 40 entries: 20 users and 20 groups.</p> |
| Available users | <p>Lists the users that match the filter value, up to the search limit value, who are not assigned to an IBM zAware role. You can sort the list by clicking the list header.</p> |
| Current mapped users | <p>Lists the users who are assigned to the selected IBM zAware role. You can sort the list by clicking the list header.</p> |

Table 34. Items displayed in the Role Mapping tab (continued)

| Item | Description |
|-----------------------|--|
| Available groups | Lists the groups that match the filter value, up to the search limit value, that are not assigned to an IBM zAware role. You can sort the list by clicking the list header. |
| Current mapped groups | Lists the groups that are assigned to the selected IBM zAware role. You can sort the list by clicking the list header. |
| Buttons | <p>Provides the following buttons:</p> <p>Add Moves the selected users or groups from the Available users or groups list to the Current mapped users or groups list.</p> <p>Add All Moves all the users or groups from the Available users or groups list to the Current mapped users or groups list.</p> <p>Apply Saves the changes you made to the role mappings.</p> <p>Remove Moves the selected users or groups from the Current mapped users or groups list to the Available users or groups list.</p> <p>Remove All Moves all the users or groups from the Current mapped users or groups list to the Available users or groups list.</p> <p>Restore Restores role mappings to the values that were in effect before you made any changes, only if you have not already clicked Apply to save your changes.</p> <p>Search Searches for user and group entries that match the specified search filter values, and displays entries that match the search filter value, up to the search limit value.</p> |

Apply Role Mappings window

Use the Apply Role Mappings window to review the changes you made to the role mappings and to confirm that you want to apply those changes.

For a description of the fields included in the Apply Role Mappings window, see Table 35.

To store your changes, click **Apply**. The IBM zAware GUI displays a confirmation message to indicate that the server must be restarted for the new role mappings to be applied. This process might take a considerable amount of time to complete because the server is automatically restarted with the new role mapping values. While the server is restarting, other GUI users receive *page not available* errors until the restart process is complete.

Table 35. Fields displayed in the Apply Role Mappings window

| Field | Description |
|--------------------------|---|
| Roles with changes | Lists the roles for which there are changes to be reviewed. |
| Mapping changes for role | Select the role for which you want to view changes. |
| Users to remove | Lists the users that will be removed from the selected role. |
| Users to add | Lists the users that will be added to the selected role. |
| Groups to remove | Lists the groups that will be removed from the selected role. |
| Groups to add | Lists the groups that will be added to the selected role. |

Specifying the duration of a browser session

The IBM zAware graphical user interface (GUI) allows you to configure the LTPA timeout value, which determines the duration of your browser session. By default, browser sessions time out after 12 hours (720 minutes). To modify this setting, use the **Security > LTPA Settings** tab.

Procedure

1. Expand the Administration category in the navigation pane and select **Configuration**. The Configure Settings page is displayed.
2. Click **Security > LTPA Settings** to display the **LTPA Settings** tab.
3. In the **LTPA timeout** field, specify the duration to use for a browser session in minutes. The allowable range of values is 10-525600 minutes (365 days).
4. Click **Apply** to save your changes. When you click **Apply**, the GUI displays a confirmation message to indicate that the web server must be restarted for your changes to be applied. This process might take a considerable amount of time to complete. Click **OK** to confirm that you want to apply your changes, or click **Cancel**.

Chapter 16. Managing IBM zAware operation and resources

You can accomplish most operations tasks through the IBM zAware graphical user interface (GUI). The following topics provide references when other interfaces or tools are required.

Accessing your notifications

A *notification* is a message notifying you of some occurrence in the system that requires your awareness or response. That is, a notification can be informational in nature, or it can be an error that requires a response from you. To view and manage your notifications for IBM zAware, use the Notifications page.

When you have unread notification messages, a lightning bolt icon (⚡) is displayed in the banner area near the *Log out* link. To display the Notifications page, you can click the lightning bolt icon, or you can click **Notifications** in the navigation pane. If no unread notification messages await your attention, the lightning bolt icon is not displayed.

On the Notifications page, each notification is displayed as a row in the Notification Messages table. The messages listed can be related to an action you performed, to an action that another user performed, or to independent server processing (such as automatically scheduled retraining). The list is shared across users, and is intended to inform you of activity on the system or in the IBM zAware partition.

The following information is displayed for each message:

Message ID

Provides the identifier for the message.

Message Text

Provides the text of the message.

Message Date/Time

Provides the date and the approximate time when the message was issued.

By default, IBM zAware appends the newest messages to the end of the list and preserves all notification messages until the IBM zAware is deactivated. If your user ID is assigned to the Administrator role, you can select entries in the table and use the **Remove** action to delete messages that you no longer need. You cannot undo this action.

To change the default sort, click the column headers.

To refresh the messages list, click **Refresh**.

Assigning storage devices to IBM zAware

To provide analytical data for monitored clients, IBM zAware requires continuous access to a set of Extended Count Key Data (ECKD) direct-access storage devices (DASD).

| |
|---|
| <p>Attention: The recommended practice is to configure the IBM zAware partition such that it has access to only those channel path identifiers (IDs), control units, and I/O devices that are required for network connectivity and storage. If this practice is not followed, an IBM zAware administrator might inadvertently assign storage devices that are in use by other partitions. To avoid the potential loss of critical system and application data on storage devices connected to the IBM zAware host system, make sure that you use the GUI to assign only those storage devices that are intended for IBM zAware use. Check with your storage administrator to make sure you select the appropriate storage devices to assign to the IBM zAware server.</p> |
|---|

To assign storage devices for IBM zAware to use for storing analytical data, use the **Data Storage** tab on the **Configure Settings** page. The content and controls displayed on the **Data Storage** tab are described in the following sections:

- “Estimating external storage device requirements”
- “Fields on the Data Storage tab”
- “Data Storage Devices”

To refresh the information that is displayed on the **Data Storage** tab, click **Refresh**.

Note that no storage devices are listed until you connect storage devices to the IBM zAware partition. For instructions, see Chapter 9, “Configuring network connections and storage for the IBM zAware partition,” on page 63.

Estimating external storage device requirements

IBM zAware stores the following analytical data on DASD:

- Current data from each monitored client, as well as priming data, if any.
- IBM zAware models for each monitored client.
- Analysis results for each monitored client.

- | IBM zAware sets default retention times for each of these types of analytical data and, through an
- | automated process that runs daily, removes the data when the retention time has elapsed. Your
- | installation can change these defaults through the **Administration > Configure Settings > Analytics** page in the IBM zAware GUI.

Storage requirements vary depending on the retention times for each type of analytical data and on the number of monitored systems that you plan to connect to IBM zAware. Start with 500 GB of storage for IBM zAware to use, plus 4-5 GB of storage for each monitored system.

If you increase the number of monitored clients, you need to configure an additional 4-5 GB of storage for each monitored system. If you increase the retention times of instrumentation data, training models, or analysis results, you also might need to increase the amount of persistent storage that IBM zAware can use. To determine whether you need to add storage devices, periodically use the **Administration > Configuration > Data Storage** page to monitor the list of assigned storage devices, their current status, and capacity.

Fields on the Data Storage tab

Table 36 provides a description of the fields that are displayed on the **Data Storage** tab.

Table 36. Fields on the Data Storage tab

| Field | Description |
|-------------------------|--|
| Total capacity (GB) | Specifies the total capacity, in gigabytes (GB), of all the storage devices that are assigned to IBM zAware. |
| Total storage used (GB) | Specifies the total amount of space, in gigabytes, that IBM zAware has allocated on the storage devices. |
| Total storage used (%) | Specifies the percentage of the total capacity that is currently allocated (in use). |

Data Storage Devices

The Data Storage Devices table lists the storage devices that are available and connected to the IBM zAware partition. Table 37 on page 145 provides a description of the columns in the Data Storage Devices table.

To sort the data in the table, click the column header for the appropriate column.

For more details about the **Add and Remove Devices** and the **Apply Pending Removals** actions, see “Adding and removing storage devices.”

Table 37. Columns in the Data Storage Devices table

| Column | Description |
|---------------|--|
| Device | Provides, in hexadecimal, the device number or unit address assigned to the device upon which the volume is mounted. |
| Status | <p>Provides the status of the device. Possible values are:</p> <p>Available Indicates that the device is not assigned to the IBM zAware server. Although the device is identified as available, it might be in use by another operating system or another IBM zAware server. Before assigning devices to the IBM zAware server, check with your storage administrator to make sure you select the appropriate storage devices.</p> <p>Being Added Indicates that the IBM zAware server is formatting the device and preparing it for use.</p> <p>In Use Indicates that the device is assigned to the IBM zAware server.</p> <p>Being Removed Indicates that the IBM zAware server is in the process of removing the device.</p> <p>Pending Removal Indicates that you selected to remove the device but IBM zAware was unable to immediately remove it. To complete the removal process, click Apply Pending Removals on the Data Storage tab. When the removal operation is complete, IBM zAware changes the status to <i>Available</i>.</p> |
| Device Type | Provides the type of device upon which the volume is mounted. |
| Capacity (GB) | Provides the size of the volume in gigabytes. If the value in the Status column is <i>Available</i> , a dash (-) is displayed in the Capacity column. |

Adding and removing storage devices

To assign storage devices for the IBM zAware server to use for storing analysis results, system behavior models, and data from monitored systems, click **Add and Remove Devices** on the **Data Storage** tab on the Configure Settings page. You can also click **Add and Remove Devices** to unassign previously assigned storage devices.

Before you begin

Complete the following actions:

- Connect storage devices to the IBM zAware partition. For instructions, see Chapter 9, “Configuring network connections and storage for the IBM zAware partition,” on page 63.
- Check with your storage administrator to make sure that you know which specific storage devices you can assign to the IBM zAware server, and the intended use (normal operations or backup) for these devices.
 - The recommended practice is to configure the IBM zAware partition such that it has access to only those channel path identifiers (IDs), control units, and I/O devices that are required for network connectivity and storage. If this practice is not followed, an IBM zAware administrator might inadvertently assign storage devices that are in use by other partitions. To avoid the potential loss of

critical system and application data on storage devices connected to the IBM zAware host system, make sure that you use the GUI to assign only those storage devices that are intended for IBM zAware use.

- If any devices are to be used for storing backup copies of IBM zAware data, your installation must define two physically separate but equivalent sets of storage devices:
 - One set for IBM zAware to use for normal operations.
 - Another set for storing backup copies of data.

The number of storage devices in each set must match, and each backup device must be equivalent in size to the device from which the data is copied. These number and size requirements also apply for configurations that contain primary and alternate IBM zAware partitions. When you use the GUI to assign a backup storage device to the IBM zAware configuration, you must use the **Preserve data** option, which prevents IBM zAware from overwriting data on the device to be added.

- Check with your storage administrator to confirm that sufficient storage will remain if you remove a device. Otherwise, IBM zAware might not have sufficient capacity to store data for monitored systems.
- Click **Refresh** to ensure that you are viewing the most recent information.

Procedure

1. To display the Configure Settings page, expand the Administration category in the navigation pane and select **Configuration**.
 2. Click the **Data Storage** tab.
 3. In the Data Storage Devices table, click **Add and Remove Devices**. The Add and Remove Devices window opens.
 4. To add one or more storage devices for the IBM zAware server to use, complete the following steps.
 - a. Only if you are adding storage devices that contain backup copies of IBM zAware data, click the **Preserve data** option, which prevents IBM zAware from overwriting data on the devices to be added.
 - b. Select one or more devices in the **Devices Available** list.
 - c. Click **Add** to move the devices to the **Devices In Use** list.
- As an alternative, you can use **Add All** to move all the devices to the **Devices In Use** list.

Attention: Do not use **Add All** if any of the available storage devices are shared. If a device is shared and in use by another application, data will be lost or overwritten if the IBM zAware server formats the device.

5. To remove a storage device that the IBM zAware server is currently using, complete one of the following actions:
 - a. Select one or more devices in the **Devices In Use** list.
 - b. Click **Remove** to move the devices to the **Devices Available** list.
- As an alternative, you can use **Remove All** to move all the devices to the **Devices Available** list.

Attention: IBM zAware rejects any attempt to reduce storage below the amount that is currently in use by the server, unless you selected all in-use devices for removal. Removing all in-use devices is a destructive operation because all stored data is deleted and IBM zAware is no longer able to provide analytical data for any monitored clients.

6. Click **OK**.

Results

The IBM zAware server completes the following actions:

- Unless you selected the **Preserve data** option, the IBM zAware server formats the devices that were moved to the **Devices In Use** list. While the formatting is in progress, the device status is *Being Added*.

Depending on the number of devices that you assign, this formatting process might take some time to complete. Periodically click **Refresh** to update the information in the Data Storage Devices table. When the formatting process is complete, the device status is *In Use*. As part of the formatting process, the volume serial (VOLSER) for the device is renamed.

- For devices that were moved to the **Devices Available** list, the IBM zAware server changes the status to *Being Removed* or *Pending Removal*, if the device cannot be removed immediately. To complete the removal process, click **Apply Pending Removals** on the **Data Storage** tab. IBM zAware unassigns the device, moves the data currently stored on the device to a device that is in use, and changes the device status to *Available*.

Important: Removing a device requires IBM zAware to recycle the analytics engine. While the removal is in progress, only the System Status page is available. When the removal process completes, you must reconnect your monitored systems to the IBM zAware server. For more details, see “Starting and stopping data collection for your monitored systems” on page 153.

Add and Remove Devices window

You can use the Add and Remove Devices window to assign storage devices to the IBM zAware server for use and to remove previously assigned devices.

To display the Add and Remove Devices window, select **Add and Remove Devices** in the Data Storage Devices table on the **Data Storage** tab.

For a description of the items that are displayed in the Add and Remove Devices window, see Table 38.

For more details about adding and removing devices, see “Adding and removing storage devices” on page 145.

Table 38. Items displayed in the Add and Remove Devices window

| Item | Description |
|-----------------------------|---|
| Preserve data option | Prevents IBM zAware from overwriting data on the device to be added. Use this option only when assigning a storage device that contains a backup copy of IBM zAware data. |
| Devices Available | Lists the storage devices that are not assigned to the IBM zAware server. |
| Devices In Use | Lists the storage devices that are currently assigned to the IBM zAware server. |

Table 38. Items displayed in the Add and Remove Devices window (continued)

| Item | Description |
|---------|--|
| Buttons | Add Use to move one or more individual devices from the Devices Available list to the Devices In Use list. |
| | Add All Use with caution. This button moves all devices in the Devices Available list to the Devices In Use list. After you click OK , IBM zAware formats and initializes the devices to be added. Unless these storage devices have been configured in the IODF for the exclusive use of IBM zAware, initializing these devices might result in the loss of data that other applications use. This button is not recommended for adding storage devices that contain backup copies of IBM zAware data. |
| | Remove Use to move one or more individual devices from the Devices In Use list to the Devices Available list. After you click OK , IBM zAware moves data that is stored on these devices to any devices that are currently in use. |
| | Remove All Use with caution. This button moves all devices in the Devices In Use list to the Devices Available list. After you click OK , IBM zAware removes all data from these devices and is no longer able to provide analytical data for any monitored clients. |
| | OK Initiates the add or remove request and closes the window. |
| | Reset Discards your selections and keeps the window open. |
| | Cancel Discards your selections, cancels the action, and closes the window. |

Specifying settings for the analytics engine

The *analytics engine* is the component of IBM zAware that manages the logstream data the server receives from each monitored system. Management actions include reading, storing, processing, and analyzing the logstream data and determining when to build new models for each monitored system. You can use the **Analytics** tab on the Configure Settings page to view the configuration values that control the analytics engine.

Table 39 on page 149 describes the fields that are displayed on the **Analytics** tab. Each field contains default values that represent reasonable estimates for IBM zAware analytics. These estimates might not be appropriate for monitored systems at your installation, so you might need to change the default values according to your knowledge of system workloads.

If you increase the retention times of instrumentation data, training models, or analysis results, you might need to increase the amount of persistent storage that IBM zAware can use. To determine whether you need to add storage devices, periodically use the **Data Storage** tab to monitor the list of assigned storage devices, their current status, and capacity.

The values on the **Analytics** tab are global settings that apply for all monitored systems. You cannot specify different date ranges for individual monitored systems but you can manage the training dates used for each monitored system through the Training Sets page. For more details, see Chapter 17, “Managing the training for monitored clients,” on page 159.

If you modify the configuration values, click **Apply** to store them. For new training period and training interval values to take effect for currently connected clients, you need to stop and reconnect those clients. For instructions, see “Starting and stopping data collection for your monitored systems” on page 153.

To undo any changes that you have not applied, click **Restore**.

Table 39. Fields on the Analytics tab

| Field | Description |
|-------------------------------------|---|
| Instrumentation data retention time | <p>Specifies the number of consecutive calendar days for which the IBM zAware server keeps the data received from monitored clients. This data provides the source for training models so the retention time must match or exceed the duration specified for Training period.</p> <p>For example, if you specify 90 days:</p> <ul style="list-style-type: none"> • The server stores client data for 90 consecutive days, whether or not instrumentation data is available on each of the days between that date range. • Periodically, the server deletes data that is older than 90 days. <p>IBM zAware uses this value to periodically remove outdated information through an automated process that runs daily.</p> <p>Default value: 365 days Valid range: 1 through 730</p> |
| Training models retention time | <p>Specifies the number of consecutive calendar days for which the IBM zAware server keeps training models for all monitored clients. If you enter 0 as the retention time, the server keeps only the current training model for each monitored client.</p> <p>IBM zAware uses this value to periodically remove outdated information through an automated process that runs daily.</p> <p>Default value: 365 days Valid range: 0 through 730</p> |
| Analysis results retention time | <p>Specifies the number of consecutive calendar days for which the IBM zAware server keeps analysis results for all monitored clients.</p> <p>IBM zAware uses this value to periodically remove outdated information through an automated process that runs daily.</p> <p>Default value: 365 days Valid range: 30 through 3650</p> |
| Training period | <p>Specifies the number of consecutive calendar days that the IBM zAware server uses to identify the instrumentation data to include in training models. The instrumentation data received on days during this time period serves as input for creating the model of normal system behavior for each monitored client. If the monitored clients at your installation process workloads in a six-month cycle, for example, you can change the value to 180 days.</p> <p>The server builds a training model from the instrumentation data received during this time period, whether or not data is available for each day.</p> <p>Default value: 90 days Valid range: 1 through 365</p> <p>For new a training value to take effect for currently connected clients, you need to stop and reconnect those clients. For instructions, see “Starting and stopping data collection for your monitored systems” on page 153.</p> <p>For more information about training periods, see “Understanding training periods and intervals” on page 159.</p> |

Table 39. Fields on the Analytics tab (continued)

| Field | Description |
|-------------------|--|
| Training interval | <p>Specifies the number of consecutive calendar days between automatic builds of system behavior models.</p> <p>IBM zAware uses this value to schedule automated builds only after the initial client model is built successfully. For an automated build to be scheduled, the client must be connected to the IBM zAware server.</p> <p>Default value: 30 days Valid range: 7 through 365</p> <p>For new a training value to take effect for currently connected clients, you need to stop and reconnect those clients. For instructions, see “Starting and stopping data collection for your monitored systems” on page 153.</p> <p>For more information about training intervals, see “Understanding training periods and intervals” on page 159.</p> |

Viewing the status of monitored clients

A *monitored client* is a z/OS system that is configured to send operations log (OPERLOG) and system log (SYSLOG) data to the IBM zAware server for analysis. To view the status of the systems that IBM zAware is monitoring, use the System Status page.

Before you begin

To ensure that you are viewing the most recent status information, click **Refresh**.

Procedure

1. To display the System Status page, select **System Status** in the navigation pane.
2. In the **Analytics engine status** field, verify that the analytics engine is running. If the status is not *Running*, IBM zAware is not collecting data from or analyzing data for the monitored systems.
3. In the zAware Monitored System Data Suppliers table, do the following:
 - View the list of systems that are or were connected to the IBM zAware server.
 - Use the Status column and the Connect Start Time column to determine which systems are connected to (*Active*) or disconnected from (*Inactive*) the IBM zAware server and to determine when the current or last connection started.
 - Use the Instrumentation Data Type column to identify from where the monitored system is retrieving the data it is supplying to the IBM zAware server.

System Status page

You can use the System Status page provided in IBM zAware to view information about the z/OS monitored systems that are or were previously connected to the IBM zAware server, to verify that the analytics engine is running, and, if your user ID is assigned to the Administrator role, to stop or start the analytics engine.

To display the System Status page, click **System Status** in the navigation pane. The controls and content displayed on the System Status page are described in the following sections:

- “About the analytics engine” on page 151
- “About monitored clients” on page 152

To display the most recent status for the analytics engine and the monitored systems, click **Refresh**.

About the analytics engine

The *analytics engine* is the component of IBM zAware that manages the logstream data the server receives from each monitored system. Management actions include reading, storing, processing, and analyzing the logstream data and determining when to build new models for each monitored system.

The System Status page provides controls that IBM zAware administrators can use to start (▶) or stop (■) the analytics engine. **Start** is enabled when the engine is stopped. **Stop** is enabled when the engine is running. Both buttons are disabled when the engine is quiesced or unavailable.

IBM zAware recycles the engine when you perform actions that require the engine to update the database where it stores the data. Such actions include assigning priming data to a sysplex, modifying the sysplex topology, or removing storage devices. You must explicitly recycle the analytics engine only after you modify the analytics configuration values, such as the training period or training interval. As an alternative to explicitly recycling the analytics engine, you can reconnect all monitored clients for your configuration changes to take effect.

When the analytics engine is stopped or recycled, IBM zAware disconnects all monitored systems from the server. When z/OS monitored clients are disconnected from the server, they automatically attempt to reconnect and continue to buffer data for approximately 10 minutes. If the analytics engine is restarted within that time, the z/OS system reconnects and sends the buffered data to the IBM zAware server. If the z/OS system times out before the analytics engine is restarted, any buffered data is lost and you must manually reconnect the system. To reconnect a z/OS system, you must issue the SETLOGR command.

```
SETLOGR FORCE,ZAICONNECT,LSN=SYSPLEX.OPERLOG
```

For more details about the consequences of starting or stopping the analytics engine, see “Starting and stopping data collection for your monitored systems” on page 153.

For a description of the possible states displayed for the analytics engine, see Table 40 on page 152.

Table 40. Field on the System Status page

| Field | Description |
|-------------------------|---|
| Analytics engine status | <p>Provides the status of the analytics engine. The engine can have one of the following status:</p> <p>Quiesced Indicates that the analytics engine is temporarily not receiving logstream data from the monitored systems and that all connections between the server and its monitored systems have been disconnected because a request that requires the engine to be recycled is being processed.</p> <p>If the analytics engine was running before you issued the request, IBM zAware restarts the engine when your request completes. After the restart, you might need to reconnect the monitored systems to the IBM zAware server.</p> <p>Running Indicates that the analytics engine is managing the logstream data that the monitored systems are transferring to the IBM zAware server.</p> <p>Started Indicates that the analytics engine is started but not yet managing the logstream data that the monitored systems are transferring to the IBM zAware server.</p> <p>Status Determination Error Indicates that the IBM zAware server is unable to determine the current state of the analytics engine.</p> <p>Stopped Indicates that the analytics engine is not receiving logstream data from the monitored systems and that all connections between the server and its monitored systems have been disconnected.</p> <p>Unavailable Indicates that the analytics engine is temporarily not managing the logstream data transferred by the monitored systems and that all connections between the server and its monitored systems have been disconnected because a storage configuration operation is in progress.</p> <p>If the analytics engine was running before the storage configuration operation began, IBM zAware restarts the engine when the request completes. After the restart, you might need to reconnect the monitored systems to the IBM zAware server.</p> |

About monitored clients

A *monitored client* is a z/OS system that sends SYSLOG or OPERLOG logstream data to the IBM zAware server for analysis. To detect problems, IBM zAware compares the system and application messages in these log files to a model of normal behavior for the z/OS system, and highlights anomalous results through the IBM zAware graphical user interface (GUI).

The zAware Monitored System Data Suppliers table lists the z/OS systems that IBM zAware is monitoring and provides the connection status for each system. For a description of the columns in the table, see Table 41 on page 153.

Note: Because this table also provides you a history of all the systems that have been connected to the server, no mechanism is provided that allows you or IBM zAware to remove systems from the list. That is, if you remove a monitored system from your installation or if you move a system to another sysplex, the systems are still listed in the table even though they no longer exist in your installation.

Table 41. Columns in the zAware Monitored System Data Suppliers table

| Column | Description |
|---------------------------|---|
| System | Provides the name of the monitored system. |
| Sysplex | Provides the name of the sysplex to which the monitored system belongs. |
| Status | <p>Indicates whether the system is connected to the IBM zAware server. The system can have one of the following status:</p> <p>Active Indicates that the system is connected to the IBM zAware server. The system might or might not be transmitting data to the server.</p> <p>Inactive Indicates that the system was previously connected to the IBM zAware server but is currently disconnected.</p> |
| Instrumentation Data Type | Indicates from where the monitored system is retrieving the data it is supplying to the IBM zAware server. The data source can be the system log (SYSLOG) or operations log (OPERLOG). |
| Connect Start Time | Provides the date and time the current or last connection started. |

Starting and stopping data collection for your monitored systems

To instruct the analytics engine to start or stop collecting data from your monitored systems, use the **Start** (▶) and **Stop** (■) controls provided on the System Status page. To perform the actions described in this topic, your user ID must be assigned to the Administrator role.

About this task

When you click **Stop** (■), the following occurs:

- IBM zAware stops the analytics engine for all monitored systems. That is, no new data is collected or analyzed for the monitored systems. Previously collected data and analysis results are preserved.
- IBM zAware disconnects all monitored systems from the server. That is, IBM zAware closes the connection that exists between the systems and the server.
- IBM zAware does not accept any new connections from monitored systems.

When you click **Start** (▶), IBM zAware starts the analytics engine for all monitored systems and accepts new connections from monitored systems. The systems might not be automatically reconnected. When z/OS monitored clients are disconnected from the server, they automatically attempt to reconnect and continue to buffer data for approximately 10 minutes. If the analytics engine is restarted within that time, the z/OS system reconnects and sends the buffered data to the IBM zAware server. If the z/OS system times out before the analytics engine is restarted, any buffered data is lost and you must manually reconnect the system. To reconnect a z/OS system, you must issue the SETLOGR command.

```
SETLOGR FORCE,ZAICONNECT,LSN=SYSPLEX.OPERLOG
```

When the system is reconnected, the analytics engine resumes collecting and analyzing the data that is received from the monitored systems. If the system was disconnected for an extended period of time and buffered data was lost, IBM zAware might not have enough available data to create a model, or the model might not be representative of normal system behavior. To avoid this situation, you can use the z/OS bulk load client for IBM zAware to provide the missing data to the IBM zAware server. If you do so, keep in mind that the server does not analyze priming data, so analytical data is not available for the time period during which the monitored client was disconnected. Also, the process of assigning priming data results in automatic recycling of the analytics engine and the disconnection of all monitored clients, so you need to determine whether the missing message data is worth this disruption to your IBM zAware environment.

To stop or restart the analytics engine, complete the steps that follow.

Procedure

1. To display the System Status page, select **System Status** in the navigation pane.
2. If the status in the **Analytics engine status** field is *Running*, click **Stop** to stop the analytics engine. You must explicitly recycle the analytics engine only after you modify the analytics configuration values, such as the training period or training interval.
3. If the status in the **Analytics engine status** field is *Stopped*, click **Start** to restart the analytics engine. You must restart the engine only if you explicitly stopped it. If you perform an action that requires IBM zAware to stop the analytics engine, such as assigning priming data to a sysplex, modifying the sysplex topology, or removing storage devices, IBM zAware automatically restarts the engine.
4. If the status in the **Analytics engine status** field is *Quiesced* or *Unavailable*, wait for the current operation to complete, then issue the start or stop request. Note that you must click **Refresh** to obtain the latest status. When the operation is complete, the status changes to *Running* or *Stopped*.

Monitoring processor and memory resources

You can view information about the IBM zAware partition and its use of processor and memory resources through several tools.

- The Partition Data Report section of the CPU Activity report, which is available through z/OS Resource Management Facility (RMF™), provides information about processor resources.
For more information about the Partition Data Report, see *z/OS Resource Measurement Facility™ Report Analysis*, SC33-7991.
- The System Activity display for the IBM zAware partition provides information about processor resources. To access the System Activity display, use the **Monitors Dashboard** task in the HMC for the IBM zAware host system.
- The Storage Information task provides information about current memory usage for the IBM zAware partition. The Storage Information task is available through the CPC Operational Customization tasks list in the Support Element (SE) for the IBM zAware host system.

For information about changing the processor and memory resources defined for a logical partition, see *zEnterprise System PR/SM Planning Guide*, SB10-7156.

For information about HMC and SE tasks, see the **System z HMC and SE (Version 2.12.1) Information Center** at <http://pic.dhe.ibm.com/infocenter/hwmca/v2r12m1/index.jsp>

Applying service updates for IBM zAware

Updates for IBM zAware are handled concurrently so you do not need to deactivate the IBM zAware partition or take any other explicit action to apply maintenance. The IBM zAware server is recycled as part of the concurrent maintenance process, however, and is temporarily unavailable for the few minutes required for the recycling process to complete.

When the server is recycled, any monitored clients that are connected to the IBM zAware server lose their TCP/IP connection to the server. z/OS monitored clients automatically attempt to reconnect to the server and continue to buffer data. To determine whether they have successfully reconnected after the server is recycled, check the **System Status** page in the IBM zAware GUI.

- If the system status is “Active”, the z/OS client successfully reconnected and sends data that it buffered while the IBM zAware server was not available.
- If the system status is “Inactive”, the z/OS system attempted to reconnect but timed out before the server recycling process completed. When the z/OS system encounters a connection timeout, it stops retrying and discards any data that was buffered. To reconnect the client, you need to issue the **SETLOGR** command on the z/OS system.

```
SETLOGR FORCE,ZAICONNECT,LSNAME=SYSPLEX.OPERLOG
```

For information about the **SETLOGR** command and the authority required to issue that command, see *z/OS MVS System Commands*, SA22-7627.

After the server is recycled, you might need to clear your browser cache to avoid viewing an older version of the IBM zAware GUI.

Deactivating the IBM zAware partition

The following steps describe the formal procedure for deactivating the IBM zAware partition.

1. Stop the data transmission from monitored clients. Use the **SETLOGR** command on each z/OS system to prevent the systems from attempting to reestablish the TCP/IP connection to the IBM zAware server.

SETLOGR FORCE,ZAIQUIESCE,ALL

For information about the **SETLOGR** command and the authority required to issue that command, see *z/OS MVS System Commands*, SA22-7627.

2. Deactivate the IBM zAware partition. Use the **Deactivate** task in the Hardware Management Console (HMC). For authorization requirements and other information about the **Deactivate** task, see the **System z HMC and SE (Version 2.12.1) Information Center** at <http://pic.dhe.ibm.com/infocenter/hwmca/v2r12m1/index.jsp>

Part 5. Advanced topics for managing IBM zAware

Topics in this part describe specialized management tasks for IBM zAware.

Topics covered in this part are:

- Chapter 17, “Managing the training for monitored clients,” on page 159
- Chapter 18, “Collecting priming data for IBM zAware models,” on page 179
- Chapter 19, “Modifying the sysplex topology,” on page 183
- Chapter 20, “Setting up a local repository to secure access to the IBM zAware GUI,” on page 185
- | • Chapter 21, “Setting up multiple IBM zAware partitions for switchover situations,” on page 187
- Chapter 22, “Enabling system management products to use IBM zAware data,” on page 191
- | • Chapter 23, “Troubleshooting problems in the IBM zAware environment,” on page 195
- Chapter 24, “Reporting IBM zAware problems to IBM,” on page 199

Chapter 17. Managing the training for monitored clients

Training is the process of using OPERLOG and SYSLOG data to build a model of normal system behavior for a monitored client. Training combined with pattern recognition techniques is how IBM zAware learns about the typical behavior of a specific system and its workload. IBM zAware compares the model that was created during the training with current data, which is collected in 10-minute intervals, to detect differences that might indicate a problem.

IBM zAware allows you to manage the training schedule for your monitored systems. Management actions include:

- Viewing the training schedule. For example, you can view the next scheduled training date and the dates to be included in the next period.
- Selecting the dates to exclude or re-include in a future training.
- Determining for which dates in the training period IBM zAware has or does not have data.
- Requesting training.
- Viewing the status of a training request.
- Canceling a training request.
- | • Identifying specific messages that are to be ignored during analysis for the selected monitored system.

Understanding training periods and intervals

IBM zAware uses two concepts, training periods and training intervals, to manage the training schedule for a monitored system. The *training period* is the number of consecutive calendar days that the IBM zAware server uses to identify the monitored system data to include in training models. The *training interval* is the number of consecutive calendar days between automatic builds of system behavior models.

That is, the training period is how many days of data IBM zAware needs to include in a model and the training interval is how often IBM zAware automatically recreates the model. By default, the training period is 90 days and the training interval is 30 days; therefore, every 30 days, IBM zAware automatically builds a model that contains data for the previous 90 days. To modify the default training period and training interval, use the **Administration > Configuration > Analytics** tab.

The following examples depict the relationship between the training period and the training interval. They also illustrate how the two different options for building a model impact the training schedule. The two options for building a model are: waiting for the server to build a model from data collected over a specific time period, or priming the server with prior data.

Example 1: Allowing IBM zAware to collect the data for the initial model

Figure 39 on page 160 depicts the calendar days for a sample training schedule in which IBM zAware collects the data for the initial model. In this example:

- The monitored system was initially connected to the IBM zAware server on day 1.
- The IBM zAware server built the initial model from data it collected during the first training period.
- The training period is 10 days, and the training interval is seven days. Note that these values are used for illustration purposes only. These values might not yield enough data to build a representative model for the systems in your installation.
- Only automatic training requests were made for the monitored system.

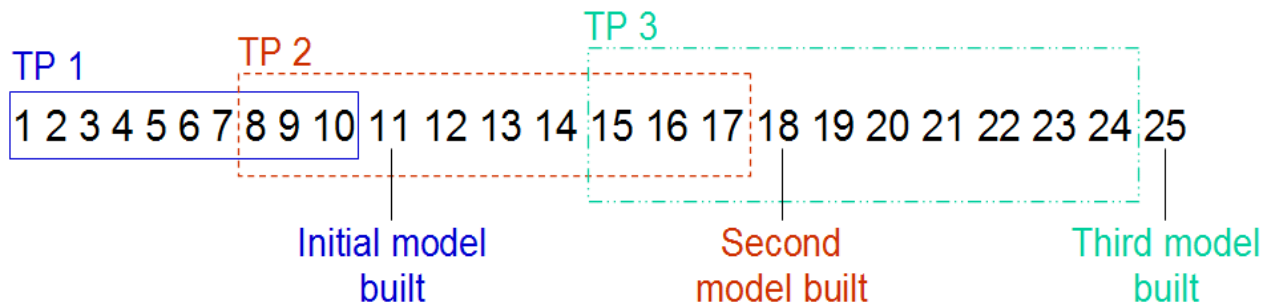


Figure 39. Training schedule for example 1

For this example, the training period dates for the initial model were from the 1st through and including the 10th. The IBM zAware server does not include data from the current day in a model; therefore, the training request (model creation) was scheduled for the 11th. For the initial model, IBM zAware does not consider the training interval. Instead, IBM zAware builds the first model the day after the first training period (TP1) ends.

IBM zAware scheduled the second training for the 18th, which is seven days (the training interval) after the initial training. Therefore, the second model includes the data that was collected from the 8th through and including the 17th. The same pattern holds true for the third training, which was scheduled for the 25th.

Note: A day begins at UTC midnight and ends at 23:59:59 UTC.

Example 2: Using priming data to build the initial model

Figure 40 depicts the calendar days for a sample training schedule in which IBM zAware uses priming data to build the initial model. In this example:

- The monitored system was initially connected to the IBM zAware server on day 1.
- IBM zAware used priming data that you provided through the z/OS bulk load client to create the initial model.
- The training period is 10 days, and the training interval is seven days. Note that these values are used for illustration purposes only. These values might not yield enough data to build a representative model for the systems in your installation.
- You requested training after the priming data was uploaded to the IBM zAware server. All other trainings were requested by IBM zAware.

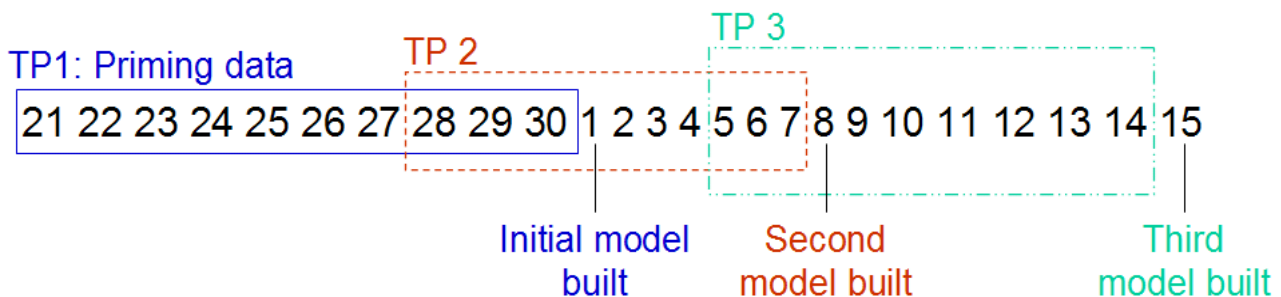


Figure 40. Training schedule for example 2

For this example, the priming data contained data for the 21st through the 30th of the previous month. You requested training on the first of the following month; therefore, IBM zAware included the priming data in the initial model.

IBM zAware scheduled the second training for the 8th, which is seven days (the training interval) after the initial training. Therefore, the second model includes the data that was collected from the 28th of the previous month through and including the 7th of the following month. The same pattern holds true for the third training, which was scheduled for the 15th.

Viewing model dates

To view model dates, use the **Manage Model Dates** action provided in the Monitored Systems table on the Training Sets page.

About this task

Through the Manage Model Dates page, you can view the information using the Summary View or the Calendar View. Through either view, you can:

- Determine the training period begin and end dates.
- View the days in the training period for which data is available, unavailable, or excluded.
- Display the date when the current model was built or when the next model is scheduled to be built.

| This topic describes how to view model dates; see “Excluding dates from a model” to learn how to
| exclude specific dates.

Procedure

1. To display the Training Sets page, expand the Administration category in the navigation pane and select **Training Sets**.
2. In the Monitored Systems table, select the system for which you want to view the model dates. You can select only one system. The system does not have to be currently connected to the IBM zAware server, but it must have been connected to the server at least once.
3. From the **Actions** list, select **Manage Model Dates**. This action is disabled if the value in the Training Progress column is *In Progress* or *In Queue*.
4. Review the information that is provided on the Manage Model Dates page. You can view the information using the Summary View or the Calendar View. To switch between the views, click **Switch to Calendar View** or **Switch to Summary View**.

Excluding dates from a model

Ideally, a model represents a predictable, stable workload that generates the same artifacts when the monitored system, its subsystems, hardware, and applications are working as your installation expects them to function. If unexpected errors or activity occurred during the training period for a monitored system, you can specify for that data to be excluded from the next model. To do so, use the **Manage Model Dates** action provided in the Monitored Systems table on the Training Sets page.

About this task

You can exclude data for dates that fall in the range of yesterday minus the training period, including the first day and yesterday. For example, if the training period is 90 days and the current date is August 8th, you can exclude dates that fall in the following range: May 9th - August 7th.

You cannot modify the current model dates. You can exclude dates only when working with the next training period model dates. After you select the dates to exclude, you can either manually request training or wait for the next scheduled training. In either case, IBM zAware builds and uses a model that excludes the selected dates.

Procedure

1. To display the Training Sets page, expand the Administration category in the navigation pane and select **Training Sets**.

2. In the Monitored Systems table, select the system for which you want to exclude dates from its model. You can select only one system. The system does not have to be currently connected to the IBM zAware server, but it must have been connected to the server at least once.
3. From the **Actions** list, select **Manage Model Dates**. This action is disabled if the value in the Training Progress column is *In Progress* or *In Queue*.
4. Complete one of the following steps:
 - To use the Manage Model Dates: Summary View to exclude dates, do the following:
 - In the **Model dates** field, select **Next Training Period Model Dates**. The content of the Manage Model Dates page changes from current model dates to model dates that apply for the next training period. You cannot exclude dates from the current model.
 - In the **Excluded dates** field, specify the date to be excluded. You can type the value; select it using the left and right arrow icons, which allow you to scroll through the dates one day or one month at a time; or select it from the calendar, which is displayed when you click the down arrow icon.
 - Click **Add** to add the date to the **Excluded Days** field.
 - Repeat this process until all the dates you want to exclude are listed in the **Excluded Days** field. If you previously excluded a date that you want to re-add to the model, in the **Excluded Days** field, select the date and click **Remove**.
 - To use the Manage Model Dates: Calendar View to exclude dates, do the following:
 - Click **Switch to Calendar View**.
 - In the **Model dates** field, select **Next Training Period Model Dates**. You cannot exclude dates from the current model.
 - In the **Training calendar** field, click the dates to be excluded. You can click any date that is not marked as unavailable. If the date will be excluded, it is surrounded by a burgundy square. If you previously excluded a date that you want to re-add to the model, click it again. The burgundy square will be removed.

Tip: To scroll backwards and forwards through the calendar by month, click the left and right arrow icons, which are displayed in the month header. To scroll backwards and forwards by year, click the first and last year link.

Results

IBM zAware excludes the selected dates when it builds the next model.

Requesting training

To request for IBM zAware to build a model of normal system behavior for a monitored system, use the **Request Training** action provided in the Monitored Systems table on the Training Sets page.

Before you begin

Verify that the IBM zAware server has received data for the number of days in the training period, which is specified on the **Administration > Configuration > Analytics** tab.

About this task

Any data that the z/OS system logger is currently sending to the IBM zAware server does not become part of the model for the monitored system until you request training or the IBM zAware server automatically builds the model. For the initial model, the server requests an automatic build when the training period elapses. For subsequent builds, the server requests an automatic build when the training interval elapses.

If you used the z/OS bulk load client to collect the data to include in the model, you can wait for the next scheduled training where the IBM zAware server will use the priming data to build the model or you can request a build. The latter option is recommended because analysis can start shortly after the model is built.

You can also consider requesting a build if you modify the software, hardware, or network configuration for a monitored system or if the workload increases on the system. When these changes occur, anomalies or new message patterns might be introduced for the system. Any differences between the model and the current data are identified on the Analysis page. After you verify that these differences are normal for the system, you might want to build a new model that includes the new message patterns or exclude this data from the model so that other differences that might indicate a potential problem are easier to identify.

- | If you are using JES3, requesting a build is also recommended after moving the JES3 global function from one system to another, through either an IPL or the dynamic system interchange (DSI) facility. After the JES3 global is moved and restarted, the message traffic on the new system contains messages that are not reflected in the existing model but are not necessarily indicative of problems. After moving the JES3 global and viewing the Analysis page results for the new system, rebuild the system model to include the JES3 messages.

If a training request completes without errors, the following occurs:

- IBM zAware creates a new model that contains all the data that was collected from the beginning of the training period to yesterday at 23:59:59 UTC. Data for the current day is not included in the model.
 - At the start of the next 10-minute interval, IBM zAware begins using the new model to identify changes in message patterns for the monitored client.
 - IBM zAware calculates the new date for the next automatic build. For example, if the training interval is 30 days, the next automatic build is scheduled for 30 days from the current date.
- | Shortly after it begins to use the new model, IBM zAware updates the next training period model dates on the Manage Model Dates page.
 - | **Note:** IBM zAware does not create a model when a training request fails. If a model existed prior to the failure, IBM zAware continues to use that model for analysis and attempts to retry the failed training request on the next day.

Procedure

1. To display the Training Sets page, expand the Administration category in the navigation pane and select **Training Sets**.
2. In the Monitored Systems table, select the system for which you want to build a new model. You can select only one system and the value in the Last Training Result column cannot be *Never Connected*. The system does not have to be currently connected to the IBM zAware server, but it must have been connected to the server at least once.
3. From the **Actions** list, select **Request Training**. This action is disabled if the value in the Training Progress column is *In Progress* or *In Queue*.
4. Click **OK** to confirm that you want to rebuild the model.

Results

A message is displayed informing you that the request was submitted or failed. If the request was submitted, the status in the Training Progress column is changed to either *In Progress* or *In Queue*. When the request completes, IBM zAware updates the Last Training Result column and the Last Training Result Time column. If the model was built, IBM zAware also updates the Current Model Built column.

Canceling training

To cancel an automatic training request or a request you submitted for a monitored system, use the **Cancel Training** action provided in the Monitored Systems table on the Training Sets page.

Procedure

1. To display the Training Sets page, expand the Administration category in the navigation pane and select **Training Sets**.
2. In the Monitored Systems table, select the system for which you want to cancel training. You can select only one system.
3. From the **Actions** list, select **Cancel Training**. This action is enabled only if the value in the Training Progress column is *In Queue*. In other words, you cannot cancel training that is already in progress.

Results

If the training request was canceled, the value in the Last Training Result column is *Cancelled* and the Last Training Result Time column is updated.

IBM zAware does not create a model when a training request is canceled. If a model existed prior to the cancellation, IBM zAware continues to use that model.

Managing ignored messages

To designate specific message IDs for IBM zAware to ignore during analysis of message data from a specific monitored system, use the **Manage Ignored Messages** action provided in the Monitored Systems table on the Training Sets page.

About this task

You can designate specific message IDs for IBM zAware to ignore during analysis. This capability is especially useful when you have recently made a change to a monitored system, such as adding a new workload. When your installation intentionally makes a significant change to a monitored system, IBM zAware might detect the resulting change in message traffic as anomalous behavior, and assign high anomaly scores to the intervals during and after the change. You can use this analysis to confirm that the anomalies are a result of expected message traffic rather than problems, and then mark the new or unusual messages as messages for IBM zAware to ignore.

You can designate messages to be ignored until the next time IBM zAware builds a model of behavior for the monitored system, or until an administrator manually changes the ignore status of the message. The ignore status for any message applies only on a per-system basis. If you want IBM zAware to ignore the same message on several monitored systems, you must repeat this procedure for setting the ignore status on each system.

You cannot identify a message to be ignored when an IBM rule already applies to that message. An IBM rule takes precedence, even when an administrator has already successfully marked the message to be ignored. This situation can occur when an administrator has successfully designated a message to be ignored, but IBM zAware later assigns an IBM rule to that message, as a result of the analysis of training data. In this case, the following conditions apply:

- For this message, the IBM rule is displayed in the Rules Status column on the Interval view.
- This message is displayed in the Ignored Messages table on the Manage Ignored Messages page, even though the IBM rule takes precedence. An administrator can remove this message from the table, but cannot successfully reapply an ignore status value to this message.

Procedure

1. To display the Training Sets page, expand the Administration category in the navigation pane and select **Training Sets**.
2. In the Monitored Systems table, select the system for which you want to manage messages. You can select only one system.
3. From the **Actions** list, select **Manage Ignored Messages**. The Manage Ignored Messages page opens, displaying the Ignored Messages table for the system that you selected.

The Ignored Messages table lists any messages that an administrator has requested IBM zAware to ignore while analyzing current data from a specific monitored client. The table is empty if an administrator has not previously designated any messages for IBM zAware to ignore during analysis.
4. To add one or more messages for IBM zAware to ignore for the selected system, complete the following steps.
 - a. Click **Add Messages** from the **Actions** list in the Ignored Messages table. The Add Ignored Messages window opens.
 - b. In the “Message IDs to ignore” field, enter one or more message IDs, separating each message ID with a comma. The message identifier (ID) must be a well-formed ID. IBM zAware recognizes messages IDs that conform to the z/OS standard, which consists of a component identifier, a message number, and an action code, in that order. IBM zAware also is capable of recognizing message IDs that do not completely conform to this z/OS standard.
 - c. Select one of the ignore status values to apply to all of the messages that you entered.

Ignore messages until next training occurs for the current system.

Marks the selected messages to be ignored during analysis until the next time IBM zAware successfully builds a model of behavior for the monitored system, as the result of either a manually requested or automatically scheduled training operation. The date and time for the next scheduled model rebuild is listed under “Next scheduled training date” after you select **Next Training Period Model Dates** on the Manage Model Dates page.

Use this value for messages that you have determined to be anomalous because of a workload change on the system, but you expect them to become part of the normal behavior for this system. The next training results in a model that includes these messages, which will be subject to normal analysis after the training.

Ignore messages until manually restored.

Marks the selected messages to be ignored during analysis until an administrator manually changes the ignore status of the message, or removes it from the list of messages in the Ignored Messages table.

Use this value for messages that you have determined to be normal (that is, not indicative of a problem) on this system. In subsequent analysis, these messages do not contribute to the anomaly score, and thus reduce false-positive results.

- d. Click **OK** to apply your changes, or click **Cancel** to return to the Manage Ignored Messages page. When you click **OK**, IBM zAware indicates whether it successfully processed the messages you entered. You can verify the results by clicking **Refresh** on the Manage Ignored Messages page, and viewing the updated list in the Ignored Messages table.
5. To change the ignore status of one or more messages in the Ignored Messages table, complete the following steps.
 - a. Select one or more messages listed in the Ignored Messages table.
 - b. Click one of the following actions from the **Actions** list in the Ignored Messages table.

These actions are equivalent to the status values described in step 4.

 - **Ignore Until Next Training**
 - **Ignore Until Manually Restored**

IBM zAware indicates whether it successfully processed the action for the messages that you selected. You can verify the results by clicking **Refresh** on the Manage Ignored Messages page, and viewing the updated list in the Ignored Messages table.

6. To remove one or more messages from the Ignored Messages table, complete the following steps.
 - a. Select one or more messages listed in the Ignored Messages table.
 - b. Click **Remove** from the **Actions** list in the Ignored Messages table. The Remove Ignored Messages window opens. This window displays a list of the messages that you selected for removal for this system.
 - c. Click **OK** to apply your changes, or click **Cancel** to return to the Manage Ignored Messages page.

When you click **OK**, IBM zAware indicates whether it successfully removed the messages that you selected. You can verify the results by clicking **Refresh** on the Manage Ignored Messages page, and viewing the updated list in the Ignored Messages table.

Training Sets page

You can use the Training Sets page provided in IBM zAware to request training for a monitored system, to display the current training status for each monitored system, and to view the current and future training dates for a monitored system.

To display the Training Sets page, expand the Administration category in the navigation pane and select **Training Sets**. The controls and content displayed on the Training Sets page are described in the following sections:

- “Monitored Systems table”
- “Actions list in the Monitored Systems table” on page 169
- “Current Training Status Details section” on page 169

Monitored Systems table

The Monitored Systems table provides the current training status for each system that is listed on the System Status page. For a description of the columns in the Monitored Systems table, see Table 42. To display the most recent training status, click **Refresh**.

Table 42. Columns in the Monitored Systems table

| Column | Description |
|---------|---|
| System | Provides the name of the monitored system. |
| Sysplex | Provides the name of the sysplex to which the monitored system belongs. |

Table 42. Columns in the Monitored Systems table (continued)

| Column | Description |
|-------------------|--|
| Training Progress | <p>Indicates the current training activity for the monitored system. One of the following values is displayed:</p> <p>In Progress Indicates that the training request is being processed.</p> <p>In Queue (n) Indicates that the training request is in the training queue and is waiting to be processed, where (n) represents the position of the request in the queue. The queue position is incremented for each subsequent request that is added to the queue.</p> <p>Because training is resource intensive, IBM zAware processes only one training request at a time. All subsequent training requests are added to the training queue and are processed in the order in which they were placed in the queue.</p> <p>"-" (dash) Indicates that there are no active or queued training requests for the monitored system.</p> <p>With the exception of the dash (-), the value in the Training Progress column is a hyperlink. Click it to expand the Current Training Status Details section, which provides additional information about the training request that was submitted for the selected monitored system.</p> |

Table 42. Columns in the Monitored Systems table (continued)

| Column | Description |
|---------------------------|--|
| Last Training Result | <p>Provides the outcome of the last training activity. One of the following values is displayed:</p> <p>Cancelled</p> <p>Indicates that the training request was canceled while it was in the training queue. IBM zAware does not create a model when a training request is canceled. If a model existed prior to the cancellation, IBM zAware continues to use that model.</p> <p>Complete</p> <p>Indicates that the last training request completed and a new model was built.</p> <p>Failed</p> <p>Indicates that the last training request failed. Typically, training requests fail for one of the following reasons:</p> <ul style="list-style-type: none"> • There is not enough data or message traffic to build a model, in which case, you may need to load more data. • An I/O error occurred. For example, IBM zAware might be unable to read or write to a file or filesystem or a filesystem might be unavailable. To resolve this issue, verify that the storage devices that are managed by IBM zAware are online and try adding storage devices for IBM zAware to use. To view and manage the storage devices, use the Administration > Configuration > Data Storage tab. <p>Note: IBM zAware does not create a model when a training request fails. If a model existed prior to the failure, IBM zAware continues to use that model for analysis and attempts to retry the failed training request on the next day.</p> <p>Never Connected</p> <p>Indicates that the monitored system has not been connected to the IBM zAware server. This result occurs under the following circumstances:</p> <ul style="list-style-type: none"> • When you use the Administration > Configuration > Priming Data tab to assign priming data for multiple systems to a sysplex, but only one of the sysplex members has been connected to the server. • When you use the Administration > Configuration > Sysplex Topology tab to move a system to a different sysplex. <p>In both cases, the IBM zAware server does not recognize the system because it identifies systems by the system and sysplex name combination. To make the IBM zAware server aware of this new system and sysplex name combination, connect the system to the IBM zAware server.</p> <p>If you used Sysplex Topology to move a system, and a model already exists for the old system and sysplex name combination, that model is preserved and is associated with the new system and sysplex name combination.</p> <p>Not Trained</p> <p>Indicates that no training has been requested for the monitored system.</p> <p>"-" (dash)</p> <p>Indicates that the result of the last training request is not available because the request is either being processed or is in the training queue.</p> <p>With the exception of the dash (-), the value in the Last Training Result column is a hyperlink. Click it to expand the Current Training Status Details section, which provides additional information about the training request that was submitted for the selected monitored system.</p> |
| Last Training Result Time | <p>Provides the date and time that the last training result was obtained. That is, the date and time the last training completed, failed, or was canceled. A dash (-) is displayed if the value in the Last Training Result column is <i>Never Connected</i> or <i>Not Trained</i> or if the value in the Training Progress column is <i>In Progress</i> or <i>In Queue</i>.</p> |
| Current Model Built | <p>Provides the date and time that the current model was built. A dash (-) is displayed if no model is available for the system.</p> |

Actions list in the Monitored Systems table

The **Actions** list provided in the Monitored Systems table lists the actions that you can take against a monitored system. Table 43 provides a description of each action and provides links to additional information that explains how to perform the action.

Table 43. Actions for monitored systems

| Action | Description | Additional Information |
|-------------------------|--|---|
| Manage Model Dates | Specify the dates to exclude from the training for the selected monitored system. View the training dates that were used to build the current model and that will be used to build the next model. | "Excluding dates from a model" on page 161 "Viewing model dates" on page 161 |
| Request Training | Build a new model of normal system behavior for the selected monitored system. | "Requesting training" on page 162 |
| Cancel Training | Cancel the training request for the selected monitored system. | "Canceling training" on page 164 |
| Manage Ignored Messages | Identify specific messages that are to be ignored during analysis for the selected monitored system. | "Managing ignored messages" on page 164 |

Current Training Status Details section

The Current Training Status Details section provides additional information about a training request. To display this information, click the link that is provided in either the Last Training Result column or the Training Progress column in the Monitored Systems table. Doing so expands the Current Training Status Details section and populates the fields with information about the training request that was submitted for the selected monitored system.

You can also expand and collapse the section by clicking the column header. If you expand the section before selecting a training request, the value for each field will be blank.

See Table 44 for a description of each field that is displayed in the Current Training Status Details section.

Table 44. Fields in the Current Training Status Details section

| Field | Description |
|-------------------|--|
| System name | Provides the name of the monitored system. |
| Training progress | Indicates the current training activity for the monitored system. One of the following values is displayed: In Progress Indicates that the training request is being processed. In Queue (n) Indicates that the training request is in the training queue and is waiting to be processed, where (n) represents the position of the request in the queue. The queue position is incremented for each subsequent request that is added to the queue. Because training is resource intensive, IBM zAware processes only one training request at a time. All subsequent training requests are added to the training queue and are processed in the order in which they were placed in the queue. "-" (dash) Indicates that there are no active or queued training requests for the monitored system. |

Table 44. Fields in the Current Training Status Details section (continued)

| Field | Description |
|---------------------------|---|
| Last training result | <p>Provides the outcome of the last training activity. One of the following values is displayed:</p> <p>Cancelled</p> <p>Indicates that the training request was canceled while it was in the training queue. IBM zAware does not create a model when a training request is canceled. If a model existed prior to the cancellation, IBM zAware continues to use that model.</p> <p>Complete</p> <p>Indicates that the last training request completed and a new model was built.</p> <p>Failed</p> <p>Indicates that the last training request failed. Typically, training requests fail for one of the following reasons:</p> <ul style="list-style-type: none"> • There is not enough data or message traffic to build a model, in which case, you may need to load more data. • An I/O error occurred. For example, IBM zAware might be unable to read or write to a file or filesystem or a filesystem might be unavailable. To resolve this issue, verify that the storage devices that are managed by IBM zAware are online and try adding storage devices for IBM zAware to use. To view and manage the storage devices, use the Administration > Configuration > Data Storage tab. <p>Note: IBM zAware does not create a model when a training request fails. If a model existed prior to the failure, IBM zAware continues to use that model for analysis and attempts to retry the failed training request on the next day.</p> <p>Never Connected</p> <p>Indicates that the monitored system has not been connected to the IBM zAware server. This result occurs under the following circumstances:</p> <ul style="list-style-type: none"> • When you use the Administration > Configuration > Priming Data tab to assign priming data for multiple systems to a sysplex, but only one of the sysplex members has been connected to the server. • When you use the Administration > Configuration > Sysplex Topology tab to move a system to a different sysplex. <p>In both cases, the IBM zAware server does not recognize the system because it identifies systems by the system and sysplex name combination. To make the IBM zAware server aware of this new system and sysplex name combination, connect the system to the IBM zAware server.</p> <p>If you used Sysplex Topology to move a system, and a model already exists for the old system and sysplex name combination, that model is preserved and is associated with the new system and sysplex name combination.</p> <p>Not Trained</p> <p>Indicates that no training has been requested for the monitored system.</p> <p>"-" (dash)</p> <p>Indicates that the result of the last training request is not available because the request is either being processed or is in the training queue.</p> |
| Training start time | Specifies the date and time the training started. The start date and time is provided only when the value in the Training Progress column is <i>In Progress</i> . Otherwise, a dash (-) is displayed. |
| Time in training (h:m:s) | Specifies the total number of hours, minutes, and seconds that IBM zAware has been processing the training request. The training length is provided only when the value in the Training Progress column is <i>In Progress</i> . Otherwise, a dash (-) is displayed. |
| Last training result time | Provides the date and time that the last training result was obtained. That is, the date and time the last training completed, failed, or was canceled. A dash (-) is displayed if the value in the Last Training Result column is <i>Never Connected</i> or <i>Not Trained</i> or if the value in the Training Progress column is <i>In Progress</i> or <i>In Queue</i> . |

Table 44. Fields in the Current Training Status Details section (continued)

| Field | Description |
|-----------------------|--|
| Entered queue time | Specifies the date and time the training request was added to the training queue. The queue time is provided only when the value in the Training Progress column is <i>In Progress</i> or <i>In Queue</i> . Otherwise, a dash (-) is displayed. |
| Time in queue (h:m:s) | Specifies the total number of hours, minutes, and seconds that the training request was or has been in the queue. The total time in the queue is provided only when the value in the Training Progress column is <i>In Progress</i> or <i>In Queue</i> . Otherwise, a dash (-) is displayed. |

Manage Model Dates page

You can use the Manage Model Dates page provided in IBM zAware to view the dates that are associated with the current model and the next training period, and you can specify which dates to exclude from the model and which dates to re-include.

To display the Manage Model Dates page, expand the Administration category in the navigation pane and select **Training Sets**. Then, invoke the **Manage Model Dates** action for a monitored system.

The Manage Model Dates page contains a Summary view and a Calendar view. The Summary view is the default view. For more details about the controls and content that are displayed in each view, see the sections that follow.

Summary view

- | The Summary view provides a text-based version of the dates that are associated with a model of system behavior. The Summary view is the default view when you navigate to the **Training Sets > Manage Model Dates** page.

The controls and content displayed in the Summary view depend on whether you select *Next Training Period Model Dates* or *Current Model Dates* in the **Model dates** field. For a description of the items that are displayed for each option, see the following sections:

- “Fields displayed for Next Training Period Model Dates”
- “Fields displayed for Current Model Dates” on page 173

To switch to a pictorial view of the model dates, click **Switch to Calendar View**. To display the Training Sets page, click **Return to Training Sets** or click the **Training Sets** breadcrumb.

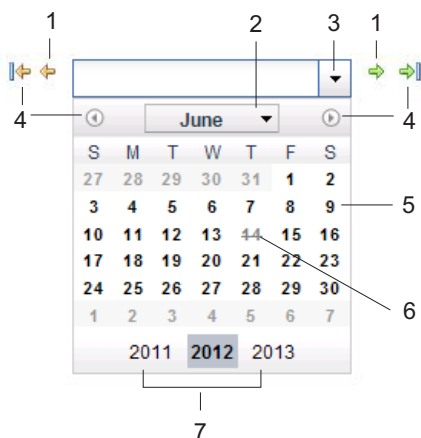
Fields displayed for Next Training Period Model Dates

When you select *Next Training Period Model Dates* in the **Model dates** field, IBM zAware displays information about the next model it will automatically build for the monitored system. For a description of the fields displayed for the next model, see Table 45.

Table 45. Fields displayed in the Summary view for the next model

| Field | Description |
|-----------------|---|
| Training system | Identifies the system for which data is displayed. The name has the format <i>sysplex-name.system-name</i> , where <i>sysplex-name</i> is the name of the sysplex to which the system belongs and <i>system-name</i> is the name of the system. |
| Model dates | Allows you to select the dates you want to view. You can select the Next Training Period Model Dates or the Current Model Dates. Depending on the value that you select for Model dates, the content of the Manage Model Dates page changes. When you display the Manage Model Dates page, Next Training Period Model Dates is selected by default. |

Table 45. Fields displayed in the Summary view for the next model (continued)

| Field | Description |
|---|--|
| Today's date (UTC) | Provides the current date in Coordinated Universal Time (UTC). |
| Manual training period begin date (UTC) | Provides the earliest date in UTC for which IBM zAware will include data when building a model in response to a training request you submit today. That is, the model will include data for dates that occurred on or between UTC midnight on the begin date through 23:59:59 UTC yesterday. |
| Next training period begin date (UTC) | Provides the earliest date in UTC for which IBM zAware will include data when automatically building the next model. That is, the model will include data for dates that occurred on or between UTC midnight on the begin date through 23:59:59 UTC on the day before the next scheduled training date. If a dash (–) is displayed in this field, the corresponding monitored system is most likely not connected to the IBM zAware server. |
| Next scheduled training date (UTC) | Provides the date in UTC when IBM zAware is scheduled to submit a request to automatically build a model. For an automated build to be scheduled, the system must be connected to the IBM zAware server. <ul style="list-style-type: none"> If a model has not been built for this system, the next training date is based on the first date for which data is available and the training period value. If a model has been built for this system, the next training date is based on the training interval value. <p>IBM zAware uses the training interval value to determine the schedule for automated builds only after the initial client model is built successfully.</p> <p>If a dash (–) is displayed in this field, the corresponding monitored system is most likely not connected to the IBM zAware server.</p> |
| Excluded dates | <p>Allows you to select dates to exclude from the model. You can type the date or select it from the calendar widget. Use the features depicted in Figure 41 to select the available dates to exclude from the model.</p>  <ul style="list-style-type: none"> 1 - Scroll by day 2 - Display the month list 3 - Display the calendar 4 - Scroll by month 5 - Dates for which data is available 6 - Dates for which data is not available 7 - Scroll by year <p>Figure 41. Features in the calendar widget</p> <p>After you specify the date to exclude, click Add to add it to the Excluded Days list.</p> <p>For more information about excluding dates, see “Excluding dates from a model” on page 161.</p> |
| Excluded Days (UTC) | Lists the dates in UTC for which IBM zAware will not include the data in the next model. To remove a date from the list, select it and click Remove . |

Fields displayed for Current Model Dates

When you select *Current Model Dates* in the **Model dates** field, IBM zAware displays information about the model it is currently using for the monitored system. For a description of the fields displayed for the current model, see Table 46.

Table 46. Fields displayed in the Summary view for the current model

| Field | Description |
|----------------------------------|---|
| Training system | Identifies the system for which data is displayed. The name has the format <i>sysplex-name.system-name</i> , where <i>sysplex-name</i> is the name of the sysplex to which the system belongs and <i>system-name</i> is the name of the system. |
| Model dates | Allows you to select the dates you want to view. You can select the Next Training Period Model Dates or the Current Model Dates. Depending on the value that you select for Model dates, the content of the Manage Model Dates page changes. When you display the Manage Model Dates page, Next Training Period Model Dates is selected by default. |
| Today's date (UTC) | Provides the current date in Coordinated Universal Time (UTC). |
| Current model trained date (UTC) | Provides the date in UTC when IBM zAware built the current model. |
| Current model begin date (UTC) | Provides the training period begin date in UTC that IBM zAware used when building the current model. That is, the current model includes data for dates that occurred on or between UTC midnight on the begin date through 23:59:59 UTC on the day before the current model trained date. |
| Excluded Days (UTC) | Lists the dates in UTC for which IBM zAware did not include the data in the current model. For more information about excluding dates, see "Excluding dates from a model" on page 161. |

Calendar view

The Calendar view provides a pictorial view of the dates that are associated with the model. To display this view, click **Switch to Calendar View** on the Summary view of the Manage Model Dates page.

The controls and content displayed in the Calendar view are described in the following sections:

- "Fields displayed in the Calendar view"
- "Understanding the training calendar" on page 174

To switch to a text-based view of the model dates, click **Switch to Summary View**. To display the Training Sets page, click **Return to Training Sets** or click the **Training Sets** breadcrumb.

Fields displayed in the Calendar view

Table 47 describes the fields that are displayed in the Calendar view.

Table 47. Fields displayed in the Calendar view

| Field | Description |
|-----------------|---|
| Training system | Identifies the system for which data is displayed. The name has the format <i>sysplex-name.system-name</i> , where <i>sysplex-name</i> is the name of the sysplex to which the system belongs and <i>system-name</i> is the name of the system. |
| Model dates | Allows you to select the dates you want to view. You can select the Next Training Period Model Dates or the Current Model Dates. Depending on the value that you select for Model dates, the content of the Manage Model Dates page changes. When you display the Manage Model Dates page, Next Training Period Model Dates is selected by default. |

Table 47. Fields displayed in the Calendar view (continued)

| Field | Description |
|-------------------|---|
| Training calendar | Uses a calendar to display the dates that are associated with the model. For more details about the training calendar, see “Understanding the training calendar.” |

Understanding the training calendar

The training calendar displays the important dates for a model using squares of different colors. For example, a green square represents the date when the next training is scheduled. Dates that are shown in a white square (without a colored outline) represent days for which IBM zAware has system data available for training purposes. For more details about the calendar, see Figure 42 and Table 48.

If Next Training Period Model Dates is selected in the **Model dates** field, you can use the training calendar to select the dates to exclude from or re-include in the next model. To exclude a date, select an available date. A burgundy box will surround the date. To re-include a date, select it again. The box will be removed.

You cannot modify the excluded dates for the current model, and you cannot use the Calendar view to modify any of the other dates for either model.

For more information about excluding dates, see “Excluding dates from a model” on page 161.

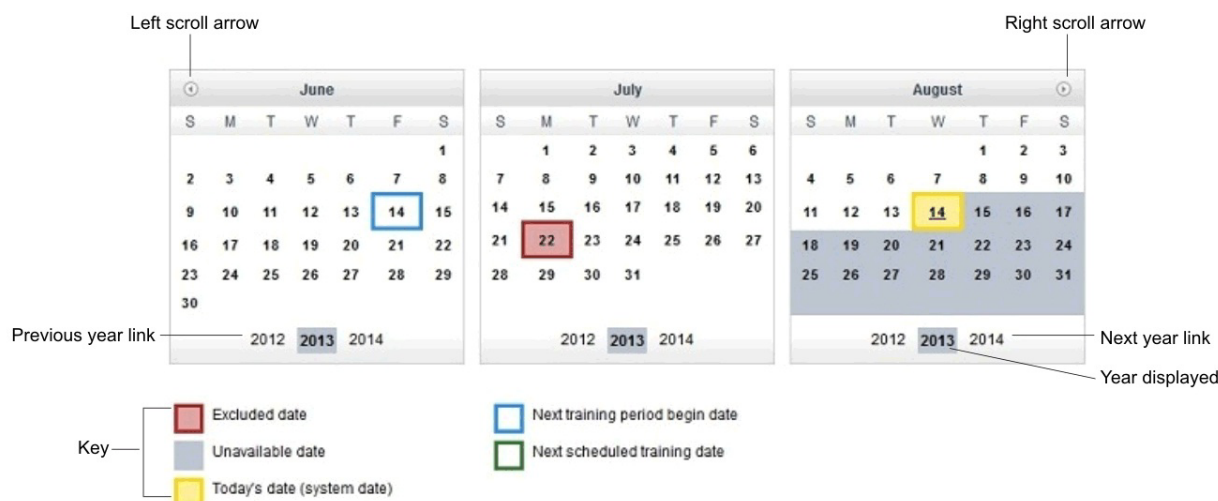


Figure 42. Training Calendar

Table 48. Items displayed in the training calendar

| Field | Description |
|--------------------|--|
| Left scroll arrow | Allows you to scroll to the previous month. |
| Right scroll arrow | Allows you to scroll to the next month. |
| Previous year link | Allows you to scroll to the previous year. |
| Next year link | Allows you to scroll to the next year. |
| Year displayed | Provides the year for which data is displayed. |

Table 48. Items displayed in the training calendar (continued)

| Field | Description |
|-------|--|
| Key | <p>Explains what the different color boxes in the calendar represent. Dates that are shown in a white square (without a colored outline) represent days for which IBM zAware has system data available for training purposes. The colors can represent one of the following dates:</p> <p>Current model begin date (purple square) The training period begin date that IBM zAware used when building the current model. This date is displayed only when Current Model Dates is selected in the Model dates field.</p> <p>Current model trained date (orange square) The date when IBM zAware built the current model. This date is displayed only when Current Model Dates is selected in the Model dates field.</p> <p>Excluded days (burgundy square) The dates that IBM zAware excluded from the current model or that IBM zAware will exclude from the next model it builds.</p> <p>Next scheduled training date (green square) The date when IBM zAware is scheduled to submit a request to automatically build the next model. This date is displayed only when Next Training Period Model Dates is selected in the Model dates field.</p> <p>Next training period begin date (blue square) The earliest date for which IBM zAware will include data when automatically building the next model. This date is displayed only when Next Training Period Model Dates is selected in the Model dates field.</p> <p>Today's date (yellow square) The current date on the system.</p> <p>Unavailable days (gray square) The dates for which IBM zAware did not or has not received data for the monitored system.</p> |

Manage Ignored Messages page

The Manage Ignored Messages page displays the Ignored Messages table for a particular system. The Ignored Messages table lists any messages that an administrator has requested IBM zAware to ignore while analyzing current data from a specific monitored client. The table is empty if an administrator has not previously designated any messages for IBM zAware to ignore during analysis. The Actions menu provides functions for adding and removing messages, and for modifying the ignore status value for a specific message.

Figure 43 on page 176 shows a sample view of the Manage Ignored Messages page.

IBM zAware

Welcome admin

Log out

IBM

- Analysis
- Notifications
- System Status
- Administration
 - Training Sets
 - Configuration

Training Sets > Manage Ignored Messages

Help

Ignored Messages for UTCPLXCB.CB8E

The Ignored Messages table lists any messages that an administrator has requested IBM zAware to ignore while analyzing current data from a specific monitored client. These messages can be ignored until manually restored or until the client model is rebuilt; the date and time from the model rebuild is listed under the 'Next training rules update scheduled' label. The Actions menu provides functions for adding and removing messages and for modifying the 'Ignore Status' value for a specific message.

Ignored Messages

Actions

Ignore Until Next Training

Ignore Until Manually Restored

Remove...

Add Messages...

| | Ignored Status | Ignore Status Applied (UTC) |
|------------------------------------|-------------------------|-----------------------------|
| | Until next training | April 17, 2013 6:51:28 PM |
| | Until next training | April 17, 2013 6:51:23 PM |
| | Until next training | April 17, 2013 6:51:42 PM |
| <input type="checkbox"/> DSNJ001I | Until next training | April 17, 2013 6:51:02 PM |
| <input type="checkbox"/> IEF285I | Until next training | April 17, 2013 6:51:48 PM |
| <input type="checkbox"/> IEF234E | Until manually restored | April 16, 2013 11:39:10 PM |
| <input type="checkbox"/> DSNJ139I | Until next training | April 17, 2013 6:51:32 PM |
| <input type="checkbox"/> IXCH0443E | Until next training | April 17, 2013 6:51:38 PM |

Refresh

Last Refresh: Wed Apr 17 2013 14:51:50 GMT-0400 (Eastern Daylight Time)

Return to Training Sets

Figure 43. The Manage Ignored Messages page

The Manage Ignored Messages page also includes the following controls:

- Click **Refresh** to update the display contents in the Ignored Messages table.
- Click **Return to Training Sets** to close the Manage Ignored Messages page and return to the Training Sets page.

176 IBM zAware Guide

Fields displayed in the Ignored Messages table

Table 49 describes the fields that are displayed in the Ignored Messages table.

Table 49. Fields displayed in the Ignored Messages table

| Field | Description |
|-----------------------------|---|
| Actions | <p>The Actions list provides functions for adding and removing messages, and for modifying the ignore status value for a specific message. All actions except for Add Messages require that you first select one or more messages in the Ignored Messages table.</p> <p>Ignore Until Next Training Marks the selected messages to be ignored during analysis until the next time IBM zAware successfully builds a model of behavior for the monitored system, as the result of either a manually requested or automatically scheduled training operation. The date and time for the next scheduled model rebuild is listed under “Next scheduled training date” after you select Next Training Period Model Dates on the Manage Model Dates page.</p> <p>Use this value for messages that you have determined to be anomalous because of a workload change on the system, but you expect them to become part of the normal behavior for this system. The next training results in a model that includes these messages, which will be subject to normal analysis after the training.</p> <p>Ignore Until Manually Restored Marks the selected messages to be ignored during analysis until an administrator manually changes the ignore status of the message, or removes it from the list of messages in the Ignored Messages table.</p> <p>Use this value for messages that you have determined to be normal (that is, not indicative of a problem) on this system. In subsequent analysis, these messages do not contribute to the anomaly score, and thus reduce false-positive results.</p> <p>Remove Opens the Remove Ignored Messages window, which displays a list of the messages that you selected for removal for this system. Click OK to apply your changes, or click Cancel to return to the Manage Ignored Messages page.</p> <p>Add Messages Opens the Add Ignored Messages window, through which you can enter message IDs of messages to ignore for the selected system. “Add Ignored Messages window” on page 178 describes the items in this window.</p> |
| Message ID | Provides the message identifier. |
| Ignore Status | <p>Lists the ignore status for the message, which can be one of the following values:</p> <p>Until next training The message is ignored during analysis until the next time IBM zAware successfully builds a model of behavior for the monitored system, as the result of either a manually requested or automatically scheduled training operation. The date and time for the next scheduled model rebuild is listed under “Next scheduled training date” after you select Next Training Period Model Dates on the Manage Model Dates page.</p> <p>Until manually restored The message is ignored during analysis until an administrator manually changes the ignore status of the message, or removes it from the list of messages in the Ignored Messages table.</p> |
| Ignore Status Applied (UTC) | Indicates the date and time (in UTC, using the 12-hour clock) at which an administrator most recently updated the ignore status for the message. |

Add Ignored Messages window

Use the Add Ignored Messages window to enter the message IDs of messages to ignore for the selected system.

Table 50. Fields displayed in the Add Ignored Messages window

| Field | Description |
|---|---|
| Current system | Identifies the system for which IBM zAware is to ignore specific messages during its analysis of current data. |
| Message IDs to ignore | The text entry field into which you can enter one or more message IDs for IBM zAware to ignore. If you enter more than one message ID, separate each ID with a comma. The message identifier (ID) must be a well-formed ID. IBM zAware recognizes messages IDs that conform to the z/OS standard, which consists of a component identifier, a message number, and an action code, in that order. IBM zAware also is capable of recognizing message IDs that do not completely conform to this z/OS standard. |
| Ignore messages until next training occurs for the current system | <p>Marks the selected messages to be ignored during analysis until the next time IBM zAware successfully builds a model of behavior for the monitored system, as the result of either a manually requested or automatically scheduled training operation. The date and time for the next scheduled model rebuild is listed under “Next scheduled training date” after you select Next Training Period Model Dates on the Manage Model Dates page.</p> <p>Use this value for messages that you have determined to be anomalous because of a workload change on the system, but you expect them to become part of the normal behavior for this system. The next training results in a model that includes these messages, which will be subject to normal analysis after the training.</p> |
| Ignore messages until manually restored | <p>Marks the selected messages to be ignored during analysis until an administrator manually changes the ignore status of the message, or removes it from the list of messages in the Ignored Messages table.</p> <p>Use this value for messages that you have determined to be normal (that is, not indicative of a problem) on this system. In subsequent analysis, these messages do not contribute to the anomaly score, and thus reduce false-positive results.</p> |
| OK | Click OK to apply your changes. |
| Cancel | Click Cancel to return to the Manage Ignored Messages page. |

Chapter 18. Collecting priming data for IBM zAware models

An *IBM zAware model* is a description of normal behavior that an IBM zAware server generates for a specific monitored z/OS system. To provide analytical data for a monitored system, the IBM zAware server requires a model of normal system behavior to use for comparison.

When you first connect a monitored system to the IBM zAware server, you have two options for building a model:

1. Waiting for the server to build a model from data collected over a specific time period.
2. Priming the server with prior data. This priming option is recommended because analysis can start shortly after the model is built.

Waiting for the server to build a model

After your installation configures z/OS monitored systems to send data to the IBM zAware server, for option 1, no additional configuration is required because the server automatically starts receiving current data from the z/OS system logger running on the z/OS monitored systems. When the training period elapses, the IBM zAware server automatically builds the IBM zAware model.

The estimated amount of data for building the most accurate models is 90 days of data for each system. Therefore, with option 1, you have to wait for the IBM zAware server to collect data for 90 days before the IBM zAware server can build a model and use that model to start detecting system problems. Your installation can modify the number of days required for this training period, based on your knowledge of the workloads running on z/OS monitored systems. For more details, see “Specifying settings for the analytics engine” on page 148.

Transferring priming data to build a model

For option 2, instead of waiting for the IBM zAware server to collect data over the course of the training period, you can prime the server by transferring prior data from the hardcopy or system logs of monitored systems, and request the server to build a model for each system from the transferred data. To do so, configure and run the z/OS bulk load client for IBM zAware on the z/OS priming system. For instructions, see Chapter 13, “Creating an IBM zAware model for new z/OS monitored clients,” on page 99.

In contrast to data that the IBM zAware server receives from the z/OS system logger running on a monitored system, the priming data from the z/OS bulk load client does not include the name of the sysplex to which the monitored system belongs. Without the sysplex name, the IBM zAware server cannot associate the priming data with the appropriate sysplex and cannot include the data in a model.

The sections that follow explain how to associate the priming data with a sysplex.

Assigning the priming data to a sysplex

If you used the z/OS bulk load client to transfer priming data to the IBM zAware server, use the **Priming Data** tab on the Configure Settings page to assign the received priming data to the appropriate sysplex.

Before you begin

Ensure that your installation has completed the following actions:

1. Configured storage, security, and analytics for the IBM zAware server.

2. Configured z/OS monitored systems to send data to the IBM zAware server. Verify that at least one monitored system is connected to the IBM zAware server for each sysplex to which you want to assign data.
3. Configured and ran the z/OS bulk load client on the z/OS priming system.

About this task

The following steps explain how to assign priming data from monitored systems by moving those systems from the **Priming data by systems** list to the **Sysplex Topology** list on the **Priming Data** tab. You do not have to assign all systems in the list until you are ready to do so. Unassigned systems remain in the **Priming data by systems** list until you add them to the sysplex topology.

Procedure

1. Expand the Administration category in the navigation pane, and select **Configuration**. The Configure Settings page is displayed.
2. Click **Priming Data** to display the **Priming Data** tab.
3. In the **Sysplex Topology** list, select the sysplex to which you want to assign systems. You can select only one sysplex. If the sysplex to which you want to assign the system is not listed, to add it to the topology, you must configure a z/OS monitored system in that sysplex and connect it to the IBM zAware server.
4. Complete one of the following actions:
 - a. Select one or more systems in the **Priming data by systems** list and click **Add** to move those systems to the selected sysplex node in the **Sysplex Topology** list.
 - b. Click **Add All** to move all the systems listed in the **Priming data by systems** list to the selected sysplex node in the **Sysplex Topology** list.

The selected systems are displayed under the selected sysplex, with the parenthetical phrase *to be assigned* displayed after the system name. If necessary, expand the sysplex node to see the list of systems for the selected sysplex.

If the selected sysplex already contains a system with the same name as the selected system, you can still add the system to the sysplex topology. In this case, during the assign process, the IBM zAware server will merge the priming data with the data that already exists for the system.

If the selected sysplex does not contain the selected system, during the assign process, the IBM zAware server will move the data to that sysplex.

5. Repeat step 4, as needed, to move each system in the **Priming data by systems** list to the appropriate sysplex in the **Sysplex Topology** list.
6. When you have finished moving systems from the **Priming data by systems** list to the appropriate sysplex, click **Assign** to apply your changes. The Assign Priming Data window is displayed.
7. Review and confirm your changes by clicking **OK**.

Results

IBM zAware recycles the analytics engine so that your changes take effect. When the analytics engine is stopped or recycled, IBM zAware disconnects all monitored systems from the server. When z/OS monitored clients are disconnected from the server, they automatically attempt to reconnect and continue to buffer data for approximately 10 minutes. If the analytics engine is restarted within that time, the z/OS system reconnects and sends the buffered data to the IBM zAware server. If the z/OS system times out before the analytics engine is restarted, any buffered data is lost and you must manually reconnect the system. To reconnect a z/OS system, you must issue the SETLOGR command.

```
SETLOGR FORCE,ZAICONNECT,LSN=SYSPLEX.OPERLOG
```

If the IBM zAware server is processing a training request when the analytics engine must be restarted, the training request is canceled and replaced in the queue so it is the first request to be processed when the analytics engine is available again.

What to do next

To verify that the transferred data is available for the IBM zAware server to use, complete the following steps:

1. Expand the Administration category in the navigation pane and select **Training Sets** to display the Training Sets page.
2. Select the monitored system for which you transferred priming data.
3. From the **Actions** list, select **Manage Model Dates**. The Manage Model Dates page is displayed.
4. In the **Model dates** field, select **Current Model Dates**.
5. Click **Switch to Calendar View** to use the calendar to determine days for which transferred data is available. Calendar days that are not marked as *Excluded* or *Unavailable* identify the dates for which the IBM zAware server has data to use.
6. Click **Return to Training Sets** to return to the Training Sets page.
7. Repeat these steps, as needed, for each system for which data was transferred.

After you verify that the data is available for the server to use, request training for the monitored system. For instructions, see “Requesting training” on page 162.

Priming Data tab

When the IBM zAware server receives priming data from the z/OS bulk load client, the data does not include the name of the sysplex to which the monitored system belongs. Without the sysplex name, the IBM zAware server cannot associate the priming data with the appropriate sysplex and cannot include the data in a model. You can use the **Priming Data** tab on the Configure Settings page to assign the priming data to the appropriate sysplex.

For a description of the items that are displayed on the Priming Data tab, see Table 51.

Table 51. Items displayed on the Priming Data tab

| Item | Description |
|------------------------|--|
| Priming data by system | Lists the systems for which priming data is available that is not assigned to a sysplex. Because the z/OS bulk load client can send data for more than one monitored system at a time, several systems might be listed. |
| Sysplex Topology | Lists the monitored systems that are or were previously connected to the IBM zAware server and organizes that list by sysplex. If you want to make changes to the sysplex topology, complete the steps provided in Chapter 19, “Modifying the sysplex topology,” on page 183. |
| Buttons | <div>Add Moves the selected systems in the Priming data by system field to the selected sysplex in the Sysplex Topology field.</div> <div>Add All Moves all the systems in the Priming data by system field to the selected sysplex in the Sysplex Topology field.</div> <div>Assign Allows you to confirm and proceed with the assignments you specified.</div> <div>Refresh Obtains the most recent data.</div> <div>Remove Moves all the systems in the selected sysplex that are marked as <i>to be assigned</i> to the Priming data by system list.</div> <div>Remove All Moves all the systems in the Sysplex Topology field that are marked as <i>to be assigned</i> to the Priming data by system list.</div> |

Assign Priming Data window

Use the Assign Priming Data window to verify that the priming data for each monitored system is assigned to the correct sysplex and to start the priming data assignment process.

The Assign Priming Data window provides the following information:

Priming Data by System

Name of the system associated with the priming data.

Sysplex to Assign

Name of the sysplex to which the priming data will be assigned.

Review and confirm your assignments by clicking **OK**. IBM zAware restarts the analytics engine so that your changes take affect.

Chapter 19. Modifying the sysplex topology

The IBM zAware server dynamically discovers and provides sysplex topology information for all the z/OS systems it monitors. If you change your sysplex topology, such as moving a system to a different sysplex, you need to modify the IBM zAware sysplex topology accordingly. To modify the sysplex topology for your monitored systems, use the **Sysplex Topology** tab on the Configure Settings page.

Before you begin

Ensure that at least one system is or was previously connected to the IBM zAware server. Otherwise, the sysplex topology display is empty.

About this task

The IBM zAware server receives OPERLOG or SYSLOG data from the z/OS system logger running on a monitored system. The server processes the log data and extracts the name of the system and the name of the sysplex to which the monitored system belongs. The server uses the system and sysplex name to:

- Uniquely identify a monitored system.
- Associate log data, models, and analytic data with the correct system.
- Build the sysplex topology.

The system name and sysplex name must uniquely identify the system to be monitored. IBM zAware identifies each monitored client by sysplex and system name, in the format *sysplex_name.system_name*; for example: SYSPLEX1.SYSA. IBM zAware cannot monitor more than one system with the same sysplex and system name combination.

Note that the priming data from the z/OS bulk load client does not include the sysplex name; therefore, you must use the **Priming Data** tab on the Configure Settings page to assign the priming data, if any, to the correct sysplex. After you assign the priming data, the IBM zAware server updates the sysplex topology.

If your installation moves a system to another sysplex, you must do the following:

- Update the sysplex topology through the IBM zAware GUI. For example, if your installation moved SYS1 from SYSPLEXB to SYSPLEXC, you also need to move SYS1 from SYSPLEXB to SYSPLEXC in the IBM zAware sysplex topology. Doing so instructs IBM zAware to associate the model and training sets information that it collected for SYSPLEXB.SYS1 with SYSPLEXC.SYS1. However, the analysis results for prior dates are not associated with SYSPLEXC.SYS1.
- Connect the system to the IBM zAware server.

To move a system from one sysplex node in the topology to another sysplex node, complete the steps that follow.

Procedure

1. Expand the Administration category in the navigation pane and select **Configuration**. The Configure Settings page is displayed.
2. Click **Sysplex Topology** to display the **Sysplex Topology** tab.
3. In the **Sysplex Topology** field, expand the sysplex node that contains the system to be moved.
4. Select the system to be moved.
5. Repeat this process until all the systems to be moved are selected.
6. Click **Move Selected Systems**. The Move Selected Systems window opens.

7. In the **Available sysplexes** field, select the sysplex to which you want to move the systems identified in the **Selected systems** field. You can select only one sysplex.
8. Click **OK** to update the topology.

Results

IBM zAware recycles the analytics engine so that your changes take effect. When the analytics engine is stopped or recycled, IBM zAware disconnects all monitored systems from the server. When z/OS monitored clients are disconnected from the server, they automatically attempt to reconnect and continue to buffer data for approximately 10 minutes. If the analytics engine is restarted within that time, the z/OS system reconnects and sends the buffered data to the IBM zAware server. If the z/OS system times out before the analytics engine is restarted, any buffered data is lost and you must manually reconnect the system. To reconnect a z/OS system, you must issue the SETLOGR command.

```
SETLOGR FORCE,ZAICONNECT,LSN=SYSPLEX.OPERLOG
```

If the IBM zAware server is processing a training request when the analytics engine must be restarted, the training request is canceled and replaced in the queue so it is the first request to be processed when the analytics engine is available again.

Move Selected Systems window

Use the Move Selected Systems window to select the sysplex to which you want to move the selected systems.

In the Move Selected Systems window, the following information is displayed:

Selected systems

Lists the systems that you selected on the **Sysplex Topology** tab. These systems will be moved to the sysplex you select in the **Available sysplexes** field.

Available sysplexes

Lists the sysplexes to which one or more monitored systems belong. Select the sysplex to associate with the systems specified in the **Selected systems** field.

Click **OK** to update the sysplex topology.

The IBM zAware server will recycle the analytics engine so that your changes can take affect. When the server restarts the engine, you must reconnect your monitored systems to the server. For more details, see “Starting and stopping data collection for your monitored systems” on page 153.

Chapter 20. Setting up a local repository to secure access to the IBM zAware GUI

Your installation has the option to provide user authentication to the IBM zAware graphical user interface (GUI) through either an existing Lightweight Directory Access Protocol (LDAP) repository or a local file-based repository. For simplicity, using an LDAP repository only is the preferred option. However, you might want to define one or two user IDs in a local repository so you can access the IBM zAware GUI when the LDAP server is unavailable. If you configure an LDAP repository and also define users or groups in a local repository, both sets of users or groups are available through the IBM zAware GUI. Use this procedure to add users or groups to a local file-based repository.

Before you begin

- To define users or groups to the local repository, you need to know the IP address or host name of the WebSphere Application Server through which you can log in to the Integrated Solutions Console. For example:
`https://server_ip_address/ibm/console` or `https://host_name/ibm/console`
- You also need to log in to the console with a user ID that has the appropriate authority to add or define users or groups. This user ID can be the default master user ID and password that was defined as part of the procedure in Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67, or another user ID that is assigned to the IBM zAware Administrator role.
- Make sure that you have reviewed the planning considerations in Chapter 6, “Planning for security,” on page 51.
- Prepare a list of user IDs or groups to define in the local repository. Do **not** define the same user ID in more than one repository; results are unpredictable.

About this task

To define users or groups to the local repository, you need use the WebSphere Application Server Integrated Solutions Console.

Attention: Do not perform any operations other than user and group management through the Integrated Solutions Console. In particular, do not change any options under the Security section, including changes related to LDAP configuration. Configuration changes in these areas do not persist across activations of the IBM zAware partition and thus might cause the loss of IBM zAware functions.

To configure an existing LDAP repository for user authentication, see Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79 for instructions.

Procedure

1. Log in to the Integrated Solutions Console, providing a user ID and password for a user assigned to the IBM zAware Administrator role.
2. In the navigation tree, select **Users and Groups**.
3. Define one or more new users in the local repository.
 - a. Click **Manage Users**.
 - b. Click **Create** and supply the required information for the new user on the Create a User page.
 - c. Optional: Click **Group Membership** to assign the user to a group.
 - 1) Optionally, supply a group name filter.
 - 2) Click **Search** to search for defined groups that match the filter.
 - 3) Select one or more groups to which you want to assign the new user, and click **Add**.

- 4) Click **Close** to return to the Create a User page.
- d. Click **Create**.
- e. Repeat these steps, as necessary, to create additional users.
4. Optional: Define one or more new groups to the local repository:
 - a. Click **Manage Groups**.
 - b. Click **Create** and supply the required information for the new group.
 - c. Click **Create**.
 - d. Repeat these steps, as necessary, to create additional groups.

Results

The user IDs and passwords that you added are defined to the local repository. If you deleted any users or groups, those users or groups have been removed from the local repository.

What to do next

- Use the instructions in “Assigning users or groups to a role” on page 137 to assign each user ID or group in the local repository to a specific IBM zAware role.
- If you need to delete a user or group from the local repository, complete the following steps.
 1. In the navigation tree of the Integrated Solutions Console, select **Users and Groups**.
 2. Click **Manage Users** or **Manage Groups**, depending on whether you need to delete a user or group.
 3. Optionally, supply a filter value and click **Search** to search for defined users or groups that match the filter.
 4. Select the user or group that you want to delete and click **Delete**.
 5. Click **Delete** again to confirm the deletion.
 6. Repeat these steps, as necessary, to delete more users or groups.

Chapter 21. Setting up multiple IBM zAware partitions for switchover situations

Your installation can configure more than one IBM zAware partition, with one for normal operations and another reserved for switchover situations. This type of configuration enables you to quickly restore IBM zAware operations after a failure. The primary and alternate partitions can reside on the same IBM zAware host system (zEC12 or zBC12) or on different host systems. Use the instructions in this topic to configure an IBM zAware environment that contains primary and alternate IBM zAware partitions.

Before you begin

Read the planning information in “Planning persistent storage configuration and capacity” on page 35 before you configure a primary or alternate IBM zAware partition. The storage administrator at your installation needs to plan for and provide a list of storage devices that are reserved for use by the primary for normal operations, and a list of equivalent storage devices for the alternate to use, when necessary. The alternate set is a backup set that contains replicated data from the primary set of storage devices.

About this task

- To correctly configure the partition in which the alternate server runs, use the same IP address as you defined for the primary partition. Doing so guarantees that you cannot have multiple IBM zAware servers running simultaneously, and also eliminates the need to reconfigure the TCP/IP settings of monitored clients if you have to switch from using the primary server to the alternate server.
- To correctly configure persistent storage for primary and alternate IBM zAware partitions, your installation must define physically separate but equivalent sets of storage devices for each partition, and also set up replication to copy the content of the primary storage devices to the alternate storage devices. For data replication to be successful, the number of storage devices in the primary set must match the number of devices in the alternate set. Additionally, each alternate device must be equivalent in size to the primary device.

The primary and alternate partitions can reside on the same IBM zAware host system (zEC12 or zBC12) or on different host systems. The alternate host system might have the IBM zAware disaster recovery (DR) feature installed, but this feature is not required.

Procedure

1. Use the instructions in Chapter 9, “Configuring network connections and storage for the IBM zAware partition,” on page 63 to set up the network connections and physical storage devices for the IBM zAware environment.
Use the Hardware Configuration Definition (HCD) to define network connections and storage devices for the primary and alternate IBM zAware partitions in the input/output configuration data set (IOCDs) for the appropriate zEC12 or zBC12 CPC.
 - For network connections, make sure that both the primary and alternate IBM zAware partitions have access to the same networks.
 - For physical storage devices, the storage administrator can use image access and candidate lists for channel path definitions to allow only the IBM zAware partition to access specific devices. Using the explicit device candidate list is an alternative method of restricting access to specific devices.
 - a. Use the explicit candidate list to allow the primary IBM zAware partition to access only the set of storage devices that are intended for normal operations.
 - b. Use the explicit candidate list to allow the alternate IBM zAware partition to access only the set of storage devices that are to contain backup copies of IBM zAware data.

- c. For the purposes of replication only, allow only one z/OS partition to access both sets of storage devices.
2. Use the instructions in Chapter 10, “Configuring an image profile for the IBM zAware partition,” on page 67 to create an activation profile for the primary IBM zAware partition. Through the Hardware Management Console (HMC), make sure you select the appropriate host system for the primary IBM zAware partition.
3. Use the instructions in Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79 to configure the primary IBM zAware partition.

When you use the IBM zAware graphical user interface (GUI) to assign storage devices for the primary server, these devices become the in-use set.
4. To complete the configuration of the primary IBM zAware environment, use the instructions in Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91 and Chapter 13, “Creating an IBM zAware model for new z/OS monitored clients,” on page 99.

When you complete this step, the primary IBM zAware server is analyzing data for its connected monitored clients, and is storing information related to its operation in the in-use set of physical storage devices.
5. Set up replication to copy the contents of the in-use set of storage devices to the backup set.

For replication, your installation can consider using IBM FlashCopy or one of several Data Facility Storage Management Subsystem (DFSMS) copy services, including Extended Remote Copy (XRC) and Peer-to-Peer Remote Copy (PPRC) solutions. Another possible alternative is using DFSMSHsm to copy data, which requires deactivating the IBM zAware partition before copying data, then reactivating the partition after the copy operation completes. Non-IBM replication products also are available for use.

If you change the set of in-use devices by adding or removing devices through the GUI, make sure that you adjust replication accordingly. To successfully replace an in-use device with its equivalent backup device, the set of in-use devices must match the set of backup devices in number of devices, size of devices, and content.
6. After the contents of the in-use set of storage devices have been replicated to the backup set at least once, configure the alternate IBM zAware partition.
 - a. Disconnect the monitored clients that are sending data to the primary IBM zAware server.
 - b. Deactivate the primary IBM zAware partition.
 - c. Using the image profile for the primary IBM zAware partition as a model, create an activation profile for the alternate IBM zAware partition.
 - Select the appropriate host system for the alternate IBM zAware partition.
 - Make sure that you use the same IP address as the one you defined for the primary partition.
 - d. Activate the alternate IBM zAware partition.
7. Through the IBM zAware GUI, configure storage, security, and analytics for the alternate IBM zAware server.

The instructions in Chapter 11, “Configuring storage, security, and analytics for the IBM zAware server,” on page 79 are essentially the same for both the primary and alternate servers, with the exception of assigning storage devices. When assigning storage devices for the alternate server:

 - a. Select only those devices in the backup set that are equivalent to the devices that are currently in use by the primary server.
 - b. When adding the selected devices, use the **Preserve data** option to ensure that IBM zAware does not format or initialize these devices, so the replicated data that they contain is preserved and usable.

After the selected devices are added, they constitute the in-use set for the alternate IBM zAware server.
8. Deactivate the alternate IBM zAware partition.
9. Reactivate the primary IBM zAware partition and reconnect its monitored clients.

Results

Your installation has two partitions of IBM zAware configured for use: the primary for normal operations, and the alternate for switchover situations, should any occur.

What to do next

- When a failure occurs and the primary partition is no longer available, activate the alternate IBM zAware partition. This switchover operation is successful only if the number of devices in the primary in-use set and in the alternate backup set match.

Any z/OS monitored clients that were connected to the primary partition automatically attempt to reconnect and continue to buffer data for approximately 10 minutes. If the alternate IBM zAware partition is activated within that time, the z/OS system reconnects and sends the buffered data to the alternate IBM zAware server. If the z/OS system times out before the alternate partition is activated, any buffered data is lost and you must manually reconnect the system.

Depending on the timing of the CPC failure and the replication schedule for backing up IBM zAware data, the data on the backup set might be back-level. In this case, the alternate IBM zAware cannot provide analytical data for the dates between the last day of replication and the date and time when the administrator activated the alternate IBM zAware.
- During the course of normal operations, an administrator might need to change the set of in-use devices for the primary server by adding or removing devices through the GUI. Because the in-use set and backup set of devices must be equivalent for a switchover to be successful, the administrator also must adjust replication and the set of storage devices for the alternate server so both of the primary and alternate sets match in number of devices, size of devices, and content. If the number of devices in the in-use set and in the backup set do not match, you cannot successfully switch over to using the alternate partition.
- If you need to add, replace, or remove storage devices from the host system after initially configuring the primary and alternate partitions of IBM zAware, use the following procedures.
 - **To add a storage device**
 1. Use HCD to add the storage devices for the primary and alternate IBM zAware partitions in the input/output configuration data set (IOCDS) for the appropriate zEC12 or zBC12 CPC.
 2. Through the IBM zAware GUI, assign the new storage device to the in-use set of storage for the primary server.
 3. Update the replication method in use at your installation to copy data from the newly added storage device to its equivalent backup device.
 4. After replication occurs at least once during normal operations, update the configuration for the alternate partition of IBM zAware:
 - a. Disconnect the monitored clients that are sending data to the primary IBM zAware server.
 - b. Deactivate the primary IBM zAware partition.
 - c. Activate the alternate IBM zAware partition.
 - d. Through the IBM zAware GUI, assign the new backup device to the in-use set of storage for the alternate server.
 - e. Deactivate the alternate IBM zAware partition.
 - f. Activate the primary IBM zAware partition.
 - g. Reconnect the monitored clients to the primary IBM zAware partition.
 - **To remove a storage device**
 1. Update the replication method in use at your installation to remove the storage device and its equivalent backup device.
 2. Through the IBM zAware GUI, remove the storage device from the in-use set of storage for the primary server.
 3. After replication occurs at least once during normal operations, update the configuration for the alternate partition of IBM zAware:
 - a. Disconnect the monitored clients that are sending data to the primary IBM zAware server.

- | b. Deactivate the primary IBM zAware partition.
- | c. Activate the alternate IBM zAware partition.
- | d. Through the IBM zAware GUI, remove the backup device from the in-use set of storage for the alternate server.
- | e. Deactivate the alternate IBM zAware partition.
- | f. Activate the primary IBM zAware partition.
- | g. Reconnect the monitored clients to the primary IBM zAware partition.
- | 4. Use HCD to remove the storage devices from the IOCDs for the appropriate zEC12 or zBC12 CPC.
- |

Chapter 22. Enabling system management products to use IBM zAware data

IBM zAware provides an application programming interface (API) that system management products can use to request analytical data to display through their own graphic user interfaces. Through this API, system management products, such as IBM Tivoli OMEGAMON, can request and receive IBM zAware analytical data in XML format. This data is equivalent to the information that is available through the **Analysis** page and **Interval view** in the IBM zAware GUI.

In addition, your installation can configure the z/OS Management Facility (z/OSMF) so that users can launch the IBM zAware GUI from the z/OSMF **Links** page.

For additional details, see the following topics:

- “Integrating IBM zAware data into monitoring and alerting products”
- “Viewing the IBM zAware GUI through z/OS Management Facility” on page 193

Integrating IBM zAware data into monitoring and alerting products

Your installation can modify system management products to request and receive IBM zAware analytical data in XML format by using the IBM zAware application programming interface (API). Use this procedure as an overview for programming a system management product to issue the API and process the returned XML data.

Before you begin

- Before your program can establish a connection with the IBM zAware server, you must enable the z/OS system on which the program runs for Application Transparent Transport Layer Security (AT-TLS). For more information about AT-TLS, see *z/OS Communications Server: IP Configuration Guide*.
- To establish a connection, you need to know the IP address of the IBM zAware server. You can code your program to use the IXGQUERY service to retrieve the IP address. For more information, see *z/OS MVS Programming: Assembler Services Guide*.

You also can code your program to use the ENFREQ service to listen for ENF event code 48, which is issued for z/OS system logger configuration changes, including changes to the IBM zAware server IP address. For more information, see *z/OS MVS Programming: Authorized Assembler Services Guide*.

- The z/OS user ID under which the program runs must be added to the IBM zAware user authentication mechanism: an existing Lightweight Directory Access Protocol (LDAP) directory or a local file-based repository. This user ID must be assigned to either the User or the Administrator role through the **Administration > Configuration > Role Mapping** page in the IBM zAware GUI.

Because authentication relies on the use of cookies, your program must be configured to accept, save, and send cookies.

About this task

Through the API, the IBM zAware server provides data that is equivalent to the information displayed through the **Analysis** page and **Interval view** in the IBM zAware GUI.

For an example of a system management program that uses the IBM zAware API, see the IBM Tivoli NetView® for z/OS topic in the IBM Redbooks publication *Extending z/OS System Management Functions with IBM zAware*, SG24-8070. This Redbooks publication is available at the following URL:

| <http://www.redbooks.ibm.com/>

Procedure

1. Connect and authenticate to the IBM zAware server. Issue a POST request to the following URL. In the code example, the variable *server_IP_address* is the IP address of the IBM zAware server.

`http://server_IP_address/zAware/j_security_check`

With the POST request, supply the user ID and password for the z/OS user ID under which the program runs.

```
j_username=username
j_password=password
```

2. Issue an HTTP GET request to retrieve analytical data from IBM zAware for a specific monitored client in a specific sysplex.

Depending on the request type, you can request the interval anomaly scores for one day or details for a specific 10-minute interval.

The following code example illustrates the syntax of the GET request.

GET `https://server_ip_address/zAware/authuser/Analysis?reqtype=request_type&time=time
&plexname=sysplex_name&lparname=system_name`

In this request:

- The variable *server_IP_address* is the IP address of the IBM zAware server.
- The remaining variables are parameters for the GET request. All parameters are required, and can be specified in any order.

reqtype

Indicates what type of analytic data that you are requesting from the IBM zAware server.

LPAR

Requests analytical data for one day for one monitored client in a specific sysplex. The returned analytical data is equivalent to the information in the **Analysis** page display in the IBM zAware graphical user interface (GUI). The returned data provides interval anomaly scores for each interval since UTC midnight on the date indicated by the *time* variable. If *time* specifies the current date, the IBM zAware returns interval anomaly scores for every interval that has occurred. If *time* specifies a prior date, the IBM zAware returns interval anomaly scores for 144 intervals.

INTERVAL

Requests analytical data for a specific 10-minute time interval for one monitored client in a specific sysplex. The returned analytical data is equivalent to the information in the **Interval view** display in the IBM zAware GUI. The returned data provides details about each unique message ID that was issued during the 10-minute interval indicated by the *time* variable.

time

Indicates the date and time period for which analytical data is requested, specified in the following format:

`YYYYMMDDhhmm00`

The *hhmm00* portion is required for an INTERVAL request, and optional for an LPAR request. If you specify the time period, use 24-hour clock time.

plexname

Specifies the name of the sysplex to which the monitored client belongs.

lparname

Specifies the name of the monitored client for which analytical data is requested.

3. Receive and process the XML data that the IBM zAware server returns in response to the GET request.

On successful completion, the response is an XML document that matches the request type:

- “XML for an LPAR request” on page 215 describes the returned XML for an LPAR request.
 - “XML for an INTERVAL request” on page 218 describes the returned XML for an INTERVAL request.
4. Periodically repeat steps 2 on page 192 and 3 to provide the system management functions that you consider necessary for each monitored system.

Consider providing notifications for the following analytical data:

- An interval anomaly score of 101.
- Multiple intervals with an interval anomaly score of 101.
- A significant change in interval anomaly score from one interval to the next.
- Intervals that contain no analytical data.

Viewing the IBM zAware GUI through z/OS Management Facility

Use this procedure as an overview for configuring z/OS Management Facility (z/OSMF) so that users can access the IBM zAware graphical user interface (GUI) through the z/OSMF navigation area. The procedure for configuring z/OSMF to link to the IBM zAware GUI is the same procedure as for any other external link that you define in the z/OSMF navigation area. For details about defining external links, use the z/OSMF online help for the **Links** page.

Before you begin

- To define links for z/OSMF, you must be authorized to do so. By default, only the z/OSMF Administrator can define links.

How users are authorized to links, and whether the authorization is performed in your security management product or through the Links task, depends on the authorization mode that is in effect for your installation. For more information about authorization modes, see the topic about setting up security in *IBM z/OS Management Facility Configuration Guide*, SA38-0652.

- You need to know the URL for the IBM zAware GUI.

The URL includes the IP address or host name assigned to the IBM zAware partition:

`https://ip_address/zAware/` or `https://host_name/zAware/`

The “zAware” portion of the URL is case-sensitive.

Procedure

To display the **Links** page, expand the z/OSMF **Administration** category in the navigation area and select **Links** to begin a sequence of steps for defining links for z/OSMF.

The following list provides a summary of the steps that are described in detail in the z/OSMF online help for the **Links** page.

- Specify the link name and its location (a URL).
- Provide a system authorization facility (SAF) resource name to be used for managing user authorizations to the link.
- | • Select a z/OSMF category for the link. Suggested categories are “Links” or “Problem Determination”.
- | • Specify how the link opens in the user's browser session (the launch behavior). The recommended behavior is to open the link in a new browser window.
- | • Manage access to the link for z/OSMF users.

Results

Users can launch the IBM zAware GUI through the z/OSMF **Links** page.

Chapter 23. Troubleshooting problems in the IBM zAware environment

The topics in this chapter describe potential problems and provide suggested corrective actions.

If you experience any problems related to the IBM zAware environment, make sure that you check the following sources of diagnostic information:

- Through the Notifications page in the GUI, you can view messages that IBM zAware issues to notify you of some activity or condition that requires your awareness or response. When you have unread notification messages, a lightning bolt icon (⚡) is displayed in the banner area near the *Log out* link. On the Notifications page, each notification is displayed as a row in the Notification Messages table. The messages listed can be related to an action you performed, to an action that another user performed, or to independent server processing (such as automatically scheduled retraining). The list is shared across users, and is intended to inform you of activity on the system or in the IBM zAware partition.
- For problems with the IBM zAware partition, you also can check the hardware messages issued to the Hardware Management Console (HMC) or Support Element (SE) for the IBM zAware host system.

If you are unable to correct the problem, use the instructions in Chapter 24, “Reporting IBM zAware problems to IBM,” on page 199 to request support from IBM.

Troubleshooting problems with the IBM zAware partition

Table 52 lists problems and fixes that you might encounter with IBM zAware partition.

Table 52. Troubleshooting tips for the IBM zAware partition

| Problem | Explanation or fix |
|--|--|
| From a correctly configured z/OS system, I attempted to start sending OPERLOG data to the IBM zAware server, but the communication failed. | <p>The communication between a monitored client and IBM zAware might fail for one of the following reasons:</p> <ul style="list-style-type: none">The IBM zAware partition might have been deactivated or is in the process of being activated.The IBM zAware partition has been activated but the IBM zAware software is still initializing.The IBM zAware partition has been activated, IBM zAware is fully initialized and accessible through its GUI, but storage devices either have not yet been assigned or are still being formatted for IBM zAware use. <p>To check the status of the partition, use the HMC or SE for the IBM zAware host system. To check the status of storage devices assigned to IBM zAware, go to the Data Storage tab in the GUI.</p> |

Troubleshooting problems with the IBM zAware server and GUI

Table 53 lists some problems and fixes that you might encounter with the IBM zAware server or the GUI.

Table 53. Troubleshooting tips for browser or GUI page displays

| Problem | Explanation or fix |
|---|--|
| I cannot successfully log in with the master user ID or password for the GUI. | The master user ID and password can be changed or reset only through the image profile for the IBM zAware partition. |

Table 53. Troubleshooting tips for browser or GUI page displays (continued)

| Problem | Explanation or fix |
|---|--|
| I have been using the IBM zAware GUI for a while but now some pages are not displaying properly. | <p>To make sure the GUI displays the latest page and content:</p> <ul style="list-style-type: none"> Make sure that the browser you are using meets requirements: <ul style="list-style-type: none"> Mozilla Firefox Extended Support Release (ESR) 17 Microsoft Windows Internet Explorer 9, with compatibility mode disabled Other browsers and browser release levels might work but have not been tested; if you use them, some IBM zAware functions might not be available and page content might not display correctly. Edit your browser options to enable JavaScript, Cascading Style Sheets (CSS) and cookies, and to disable software that blocks pop-up windows, especially if you are using keyboard controls rather than the mouse to use the GUI. Clear your browser cache after applying service for IBM zAware, and periodically during normal use. |
| When I click on a link on a GUI page, such as the icon for help, nothing seems to happen. | Make sure that the browser you are using is correctly configured to enable pop-up windows to open. |
| I connected a new monitored client and the IXG messages issued on the z/OS system indicate that the connection was successful. However, the system does not appear on the System Status page, or the value shown in the Instrumentation Data Type column is not correct. | <ol style="list-style-type: none"> On the newly connected system, issue the SETLOGR command to stop data transmission: SETLOGR FORCE,ZAIQUIESCE,ALL Wait a few minutes, then issue the SETLOGR command to reconnect the client: SETLOGR FORCE,ZAICONNECT,LSNAME=SYSPLEX.OPERLOG |
| I expected to see analysis data for a particular monitored client on a specific date, but the Analysis page display does not contain a bar graph for that client and date. | <p>Analytical data might not be available for all systems for the date and time that you select for the Analysis page display. Data is not available under the following circumstances:</p> <ul style="list-style-type: none"> The monitored client is not connected and sending current data to the IBM zAware server. The monitored client was added to the sysplex topology after the date you select for the Analysis page display. <p>Note that analytical data is not available for the dates for which you supplied priming data, unless the monitored client was connected and sending data to the IBM zAware server on those dates. The server uses priming data only for creating the model of system behavior.</p> |
| I have been using the IBM zAware GUI but it now appears to be hanging. | <p>IBM zAware might have lost access to one or more of its in-use storage devices. When an in-use storage device becomes unavailable, IBM zAware operations stop. To a user of the IBM zAware GUI, the GUI appears to hang. On the SE for the IBM zAware host system, hardware messages indicate input/output (I/O) problems related to the loss of access to physical storage devices.</p> <p>See the response to message "AIFP0013E" on page 230 for instructions to diagnose and correct this condition.</p> |

Troubleshooting problems with the z/OS bulk load client for IBM zAware

Table 54 lists some problems and fixes that you might encounter with running the z/OS bulk load client to transfer priming data to the IBM zAware server.

Table 54. Troubleshooting tips for running the z/OS bulk load client for IBM zAware

| Problem | Explanation or fix |
|--|---|
| The REXX call to run the z/OS bulk load client is failing with an invalid character on line 1. | Check the TSO profile to make sure that the PACK option is set to OFF and resubmit the z/OS bulk load client job. |

Troubleshooting problems with z/OS monitored clients

Table 55 lists some problems and fixes that you might encounter with configuring and managing z/OS monitored clients. For a more comprehensive list of possible errors and fixes, see the topic on resolving z/OS IBM zAware log stream client errors in *z/OS MVS Diagnosis: Reference*, GA22-7588.

Table 55. Troubleshooting tips for z/OS monitored clients

| Problem | Explanation or fix |
|--|--|
| When configuring a z/OS system as an IBM zAware monitored client, I attempted to define or update an existing OPERLOG log stream with the ZAI and ZAIDATA parameters but the request failed with reason code "839"x. | <p>The active primary LOGR couple data set is not formatted at the level required to process the request. You can specify the ZAI and ZAIDATA keywords for a log stream only when the LOGR CDS format level is at least HBB7705.</p> <p>To determine what format level is in use for a sysplex, enter the following command and check the resulting message display.</p> <pre>D XCF,COUPLE,TYPE=LOGR</pre> <p>If the LOGR CDS format level is not HBB7705, your installation needs to run the format CDS utility IXCL1DSU with the DATA TYPE(LOGR) and ITEM NAME(SMDUPLEX) NUMBER(1) options. For additional information, see the topic on LOGR parameters for the format utility in <i>z/OS MVS Setting Up a Sysplex</i>.</p> |
| From a correctly configured z/OS system, I attempted to start sending OPERLOG data to the IBM zAware server, but the communication failed. | <p>The communication between a monitored client and IBM zAware might fail for one of the following reasons:</p> <ul style="list-style-type: none">• The IBM zAware partition might have been deactivated or is in the process of being activated.• The IBM zAware partition has been activated but the IBM zAware software is still initializing.• The IBM zAware partition has been activated, IBM zAware is fully initialized and accessible through its GUI, but storage devices either have not yet been assigned or are still being formatted for IBM zAware use. <p>To check the status of the partition, use the HMC or SE for the IBM zAware host system. To check the status of storage devices assigned to IBM zAware, go to the Data Storage tab in the GUI.</p> |

Table 55. Troubleshooting tips for z/OS monitored clients (continued)

| Problem | Explanation or fix |
|--|--|
| On a z/OS system that is established as an IBM zAware monitored client, I see repeated socket error messages. What happened to the connection between the z/OS system and the IBM zAware server? | <p>The IBM zAware analytics engine might be stopped or recycling. When the analytics engine is stopped or recycled, IBM zAware disconnects all monitored systems from the server. When z/OS monitored clients are disconnected from the server, they automatically attempt to reconnect and continue to buffer data for approximately 10 minutes. During this time, the socket error messages are issued until the z/OS system successfully reconnects or stops retrying.</p> <p>If the analytics engine is restarted within that time, the z/OS system reconnects and sends the buffered data to the IBM zAware server. If the z/OS system times out before the analytics engine is restarted, any buffered data is lost and you must manually reconnect the system. To reconnect a z/OS system, you must issue the SETLOGR command.</p> <pre>SETLOGR FORCE,ZAICONNECT,LSN=SYSPLEX.OPERLOG</pre> <p>To check the status of the IBM zAware analytics engine, go to the System Status page in the GUI.</p> |

Chapter 24. Reporting IBM zAware problems to IBM

- | If the “Call Home” feature is enabled on the IBM zAware host system (zEC12 or zBC12 CPC), Licensed Internal Code automatically gathers and sends diagnostic information to IBM when specific problems with IBM zAware are detected. For other problems, or if the “Call Home” feature is not enabled, you have to take action to report the problem to IBM Support. In either case, IBM Support receives the call and contacts you to obtain more information about the event. Use this topic to determine whether you
- | need to take action, to learn how to report a problem, and to prepare for your call with IBM Support. If
- | you do not have a maintenance contract with IBM, use the questions at the end of this topic to collect the
- | information that you might need to report the problem to your hardware maintenance provider.

Before you begin

- Note all of the problem symptoms that you have encountered with the IBM zAware partition, server, or a z/OS monitored client. For example, you might have seen network connectivity problems, partition activation failures, or error messages related to IBM zAware processing.
- Depending on the type of problem and whether the “Call Home” feature is enabled on the IBM zAware host system, determine which reporting method is appropriate. The following list describes the available reporting methods:

Hardware PMR – automatic “Call Home”

If the “Call Home” feature is enabled on the IBM zAware host system and Licensed Internal Code detects specific problems with IBM zAware, a hardware PMR is automatically generated and sent to IBM Support.

If the “Call Home” feature is enabled on the IBM zAware host system, determine whether a hardware PMR already exists for this problem. Use the Hardware Management Console (HMC) to check for outstanding hardware messages that indicate a “Call Home” call for the IBM zAware partition or the partition in which the z/OS monitored client is running.

Hardware Type V – viewable PMH (PMV)

For problems that are not detected by firmware or did not generate automatic hardware PMRs, you can request IBM support by generating a Type V Viewable PMH (PMV) record, using the instructions in this procedure.

Software PMR

If you encounter a problem that appears to be directly related to a particular software component, as opposed to the IBM zAware partition or connectivity to the IBM zAware server, you can open a Software PMR against the problematic component. If you are not sure which component is the cause of the problem, open a PMV record instead of a software PMR. After the problematic component is identified, IBM Support can transfer the problem record to the appropriate support center.

- If a hardware PMR was generated for the problem, prepare for your call with IBM Support by reviewing the questions in What to do next. Otherwise, if you need to report a problem to IBM by generating a Type V viewable PMH, complete the following steps.

About this task

The *zEnterprise System Support Element Operations Guide Version 2.12.0*, SC28-6920, provides more details about the tasks listed in the following steps.

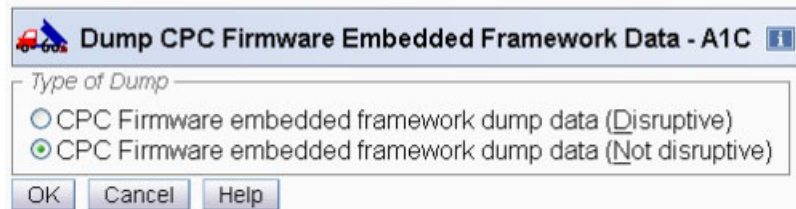
Procedure

1. Log in to the Support Element on the HMC through **Single Object Operations**, using a user ID assigned to the system programmer or service representative user role.
- | 2. Locate the object for the IBM zAware host system (zEC12 or zBC12 CPC).

- Optional: In the **Service task** list, select the **Dump LPAR data** task and use it to request a dump of the IBM zAware partition.

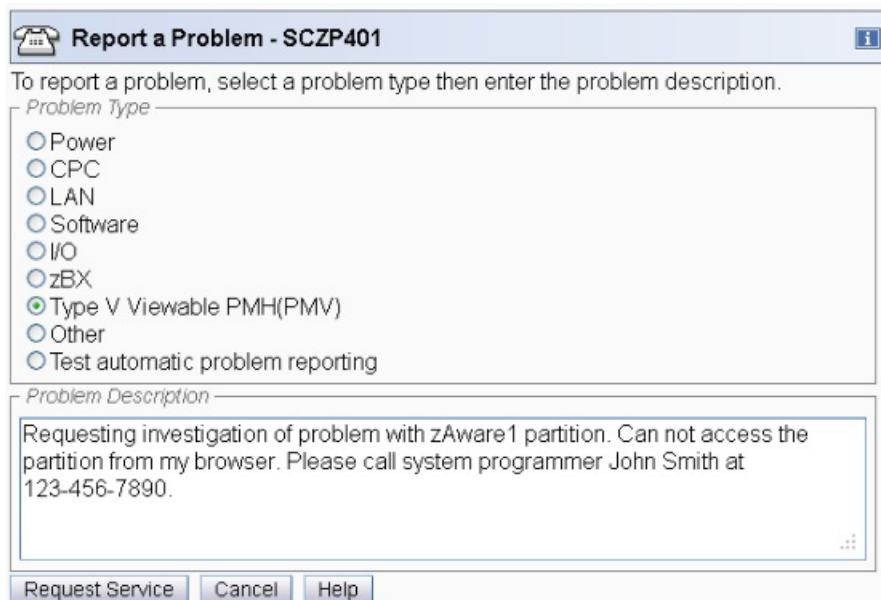
Depending on the type of problem, IBM Support might ask you to send a dump of the IBM zAware partition. You can skip this step and wait for IBM Support to tell you whether a dump is required for diagnosis.

If you decide to send a dump without direction from IBM Support, make sure you select the non-disruptive LPAR dump. Click **OK**.



- Select the **Report a problem** task to open a problem of **Type V Viewable PMH(PMV)**.

In the Problem Description text area, briefly describe the problem you have encountered and provide contact information.



- Use the **View PMV Records** task to retrieve the problem management number (PMR) for the problem report that you opened.

- If you completed step 3, use the **Transmit service data** task to send the LPAR dump to IBM Support.

Do *not* attach this data to an open problem; instead, create a new PMR.

Select the following:

- System Availability Data
- Support element logs
- Problem Determination Data
- CPC Firmware embedded framework dump data

Results

A PMV record is generated and sent to IBM Support. If you requested and transmitted a dump for the IBM zAware partition, that data is sent to IBM Support also.

What to do next

Prepare for your call with IBM Support. If you have not sent an LPAR dump for the IBM zAware partition, IBM Support might request you to do so. Depending on the type of problem, IBM Support also might request screen captures of IBM zAware partition or server configuration settings.

IBM Support also might ask you to take further action or answer one or more of the following questions:

- View the hardware messages associated with the IBM zAware partition on the host system. If any of these hardware messages are related to IBM zAware, tell IBM Support about those messages that did not generate an automatic “Call Home” hardware PMR.
- For the IBM zAware partition:
 - Are you experiencing a problem with a new IBM zAware partition that you have not yet successfully activated?
 - What is the name of the IBM zAware partition?
 - Provide details about the network interface card (NIC) and virtual local area network (VLAN).
 - Are all ZAWARE stream microcode load levels (MCLs) installed and activated?
- For a IBM zAware monitored client:
 - Is the z/OS system running in a partition on the IBM zAware host system (on the same CPC as the IBM zAware partition)?
 - What release of the z/OS operating system is installed?
- For the problem itself:
 - What are the problem symptoms? For example, dumps are taken, LPAR activation fails, training request fails, and so on.
 - Can you easily reproduce the problem or is it intermittent?
 - What is the exact date and time of the last failure?

Part 6. Appendixes

Appendix A. Summary of IBM zAware tasks and required IT skills, tools and information

- The IBM zEnterprise System (zEnterprise) product library, which includes System z hardware books, is available through **Resource Link** at <http://www.ibm.com/servers/resourcecelink>.
- The z/OS product library is available in the z/OS Internet Library web site at <http://www.ibm.com/systems/z/os/zos/bkserv/>.

Table 56. Summary of IBM zAware tasks and required IT skills, tools and information

| Task | IT role / skill | Tools / interfaces | Information resources |
|--|---|--|--|
| Plan to use IBM zAware | System planners and installation managers | — | <ul style="list-style-type: none"> • Chapter 3, “Project plan for configuring and using IBM zAware,” on page 13 • Part 2, “Planning to configure IBM zAware,” on page 17 • <i>zEnterprise EC12 System Overview</i>, SA22-1088 |
| Configure IBM hardware, networking and storage devices that support the IBM zAware partition | <ul style="list-style-type: none"> • System planners and installation managers • Network administrators • Storage administrators | Hardware Management Console (HMC) user interface (UI) | <ul style="list-style-type: none"> • Part 2, “Planning to configure IBM zAware,” on page 17 and Part 3, “Configuring IBM zAware and its monitored clients,” on page 61 • <i>zEnterprise System PR/SM Planning Guide</i>, SB10-7156 |
| Configure the IBM zAware partition | <ul style="list-style-type: none"> • Systems programmers • Network administrators • Storage administrators | HMC UI | <ul style="list-style-type: none"> • Part 3, “Configuring IBM zAware and its monitored clients,” on page 61 • <i>zEnterprise System Hardware Management Console Operations Guide for Ensembles</i>, SC27-2615 |
| Prepare the IBM zAware server for operation | <ul style="list-style-type: none"> • Systems programmers • Storage administrators • Security administrators | IBM zAware graphical user interface (GUI) or operating system interfaces | <ul style="list-style-type: none"> • Part 3, “Configuring IBM zAware and its monitored clients,” on page 61 • Books listed in Table 57 on page 206 |
| Configure operating systems to send data to the IBM zAware server | <ul style="list-style-type: none"> • Systems programmers • Network administrators | IBM zAware GUI or operating system interfaces | <ul style="list-style-type: none"> • Part 3, “Configuring IBM zAware and its monitored clients,” on page 61 • Books listed in Table 57 on page 206 |

Table 56. Summary of IBM zAware tasks and required IT skills, tools and information (continued)

| Task | IT role / skill | Tools / interfaces | Information resources |
|--|--|---|---|
| Manage the use and operation of the IBM zAware server | <ul style="list-style-type: none"> Systems programmers Network administrators Storage administrators Security administrators | IBM zAware GUI or operating system interfaces | Part 4, "Managing and using the IBM zAware server," on page 107 and Part 5, "Advanced topics for managing IBM zAware," on page 157 |
| View and interpret analytical data and resolve potential system problems | <ul style="list-style-type: none"> Systems programmers Experienced application programmers | IBM zAware GUI | <ul style="list-style-type: none"> Part 4, "Managing and using the IBM zAware server," on page 107 and Part 5, "Advanced topics for managing IBM zAware," on page 157 <i>z/OS MVS Diagnosis Reference</i> |
| Connect the IBM zAware GUI to other system management or monitoring products | <ul style="list-style-type: none"> Systems programmers Experienced application programmers | Various, depending on system management or monitoring product | Part 2, "Planning to configure IBM zAware," on page 17 and Part 4, "Managing and using the IBM zAware server," on page 107 |
| Update vendor programs that duplicate HMC/SE configuration tasks | Experienced application programmers | Various System z APIs | <ul style="list-style-type: none"> <i>System z Application Programming Interfaces</i>, SB10-7030 <i>System z API for Java</i>, API-JAVA <i>System z Hardware Management Console Web Services API</i>, SC27-2617 <i>System z CIM Management Interface</i>, SB10-7154 |
| Update vendor programs that duplicate IBM zAware functions | Experienced application programmers | | Appendix C, "Application Programming Interface (API) for monitoring products," on page 213 |

Table 57. IBM zAware information in the z/OS product library

| z/OS title and order number | IBM zAware-related content |
|---------------------------------------|---|
| <i>z/OS MVS System Commands</i> | <ul style="list-style-type: none"> Table 7. MVS Commands, RACF Access Authorities, and Resource Names DISPLAY LOGGER command DISPLAY MSGFLD command SET command (IXGCNF parameter) SETLOGR command |
| <i>z/OS Planning for Installation</i> | The APAR requirement for system logger is listed in the entry for the BCP component in Table 39. <i>Hardware requirements for z/OS V1R13 elements and features.</i> |

Table 57. IBM zAware information in the z/OS product library (continued)

| z/OS title and order number | IBM zAware-related content |
|---|--|
| <i>z/OS Setting up a Sysplex</i> | <ul style="list-style-type: none"> • Planning the IXGCNF system parameter • Planning for system logger applications <ul style="list-style-type: none"> – Define authorization for the system logger address space – Updating a log stream's attributes – Preparing for z/OS IBM zAware log stream client usage • LOGR parameters for format utility • LOGR keywords and parameters for the administrative data utility |
| <i>z/OS MVS Planning: Operations</i> | New topic: Exploiting the IBM System z Advanced Workload Analysis Reporter (IBM zAware) for OPERLOG |
| <i>z/OS MVS Programming: Assembler Services Reference, Volume 2</i> | <ul style="list-style-type: none"> • IXGINVNT — Managing the LOGR inventory couple data set • IXGQUERY — Query a log stream or system logger information |
| <i>z/OS MVS Programming: Assembler Services Guide</i> | Using system logger services: <ul style="list-style-type: none"> • IXGINVNT: Managing the LOGR policy • IXGQUERY: Get information about a log stream or system logger |
| <i>z/OS MVS Programming: Authorized Assembler Services Guide</i> | <ul style="list-style-type: none"> • Using system logger services • Setting up the system logger configuration • Writing an ENF event 48 listen exit |
| <i>z/OS Diagnosis: Reference</i> | System logger: <ul style="list-style-type: none"> • Resolving system logger z/OS IBM zAware log stream client errors |
| <i>z/OS MVS Diagnosis: Tools and Service Aids</i> | Updated topic: SYSLOGR component trace |
| <i>z/OS System Messages, Vol 1</i> | New AIZ message descriptions for messages that the z/OS bulk load client for IBM zAware issues |
| <i>z/OS System Messages, Vol 10</i> | New and updated IXG message descriptions for messages that the z/OS system logger issues |
| <i>z/OS MVS System Management Facility</i> | Updated topic: Record Type 88 (58) — System Logger Data |
| <i>z/OS Initialization and Tuning Reference</i> | <ul style="list-style-type: none"> • IEASYSxx (system parameter list): IXGCNF parameter • IXGCNFxx (system logger initialization parameters) |

Appendix B. Sample certificate authority (CA) reply

Your installation has the option of replacing the IBM zAware default SSL certificate with a certificate signed by a certificate authority of your choice. This topic provides sample certificate blocks to illustrate the content that you might receive from a certificate authority.

When you receive a reply from a certificate authority, the reply might contain a chain of certificates, starting with the signed server certificate, possibly followed by certificates from one or more intermediate CAs and, finally, the self-signed certificate of the CA. Figure 44 on page 210 provides sample certificate blocks to illustrate the content that you might receive from a certificate authority. In this sample, the reply chain consists of the following:

1. The first block of certificate is the IBM zAware server certificate, as returned by the certificate authority. This certificate is signed by the next signer in the chain.

```
subject=/C=US/ST=NY/L=Poughkeepsie/O=ibm.com/OU=SysTest/CN=9.xx.xx.xx/UID=xxx97/mail=emplye@us.ibm.com  
issuer=/C=US/O=International Business Machines Corporation/CN=IBM INTERNAL INTERMEDIATE CA
```

2. The next block of certificate text is the signer of the IBM zAware server certificate; in this sample, the signer is an intermediate certificate authority. This certificate is signed by the next signer in the chain. Note that the reply can contain one or more blocks for intermediate signers.

```
subject=/C=US/O=International Business Machines Corporation/CN=IBM INTERNAL INTERMEDIATE CA  
issuer=/C=US/O=International Business Machines Corporation/CN=IBM Internal Root CA
```

3. The final block of certificate text is the self-signed certificate for the certificate authority itself. It is self signed. This certificate must be added to the browser's trust store to authenticate the IBM zAware server.

```
subject=/C=US/O=International Business Machines Corporation/CN=IBM Internal Root CA  
issuer=/C=US/O=International Business Machines Corporation/CN=IBM Internal Root CA
```

```

subject=/C=US/ST=NY/L=Poughkeepsie/O=ibm.com/OU=SysTest/CN=9.xx.xx.xx/UID=xxx97/mail=emplye@us.ibm.com
issuer=/C=US/O=International Business Machines Corporation/CN=IBM INTERNAL INTERMEDIATE CA
-----BEGIN CERTIFICATE-----
MIIF0DCCB LIgAwIBAgICD6kwdQYJKoZIhvcNAQEFBQA wajELMAkGA1UEBhMCVVMx
NDAYBgNVBAoTK01udGVyb mF0aW9uYWwgQnVzaW5lc3MgTW FjaGl uZXMgQ29ycG9y
:
5i5BozwFbvxCdM2INWzEaejdmejdCSDkgDGqgVtXXZnZeCtREOGME99nm3fHW7h
QkyXkg==
-----END CERTIFICATE-----

subject=/C=US/O=International Business Machines Corporation/CN=IBM INTERNAL INTERMEDIATE CA
issuer=/C=US/O=International Business Machines Corporation/CN=IBM Internal Root CA
-----BEGIN CERTIFICATE-----
MIID7TCCAtWgAwIBAgIBAJANBgkqhkiG9w0BAQUFADBiMQswCQYDVQQGEwJVUzE0
MDIGA1UEChMrSW50ZXJuYXRpb25hbCBCdXNpbmVzcyBNYWNoaW5lc yBDb3Jwb3Jh
:
irUCKeSX1o3HGZFhMYw lKsYwog470qbYqDIqP+JM2N161GaNHilDcW49qKvQTkV5
fg==
-----END CERTIFICATE-----

subject=/C=US/O=International Business Machines Corporation/CN=IBM Internal Root CA
issuer=/C=US/O=International Business Machines Corporation/CN=IBM Internal Root CA
-----BEGIN CERTIFICATE-----
MIIDxCCAqygAwIBAgIBADANBgkqhkiG9w0BAQUFADBiMQswCQYDVQQGEwJVUzE0
MDIGA1UEChMrSW50ZXJuYXRpb25hbCBCdXNpbmVzcyBNYWNoaW5lc yBDb3Jwb3Jh
:
bwnogYppATaH1z2PpMC3nqhyMv6B+NfAen1iMVbAFERrDRUuPD+Rt09s8ayEwVqp
3+HY0FBqh lI=
-----END CERTIFICATE-----

```

Figure 44. Sample reply from a third-party certificate authority

When you supply this information in the GUI, provide the entire certificate chain, starting with the signed server certificate through the self-signed certificate of the CA. Make sure that you do not insert any lines or spaces between the end of one certificate and the beginning of the next certificate. Figure 45 on page 211 illustrates the correct format for pasting certificate content. In the figure, the ellipses represent certificate content that has been removed only for publication in this book. When you paste certificate replies in the GUI, make sure that you include all of the content, including the header -----BEGIN CERTIFICATE----- through and including -----END CERTIFICATE-----

```

-----BEGIN CERTIFICATE-----
MIIF0DCCBliGAWIBAgICD6kwdQYJKoZIhvcNAQEFBQAwaJELMAkGA1UEBhMCVVMx
NDAYBgNVBAoTK01udGVybmF0aW9uYWwgQnVzaW5lc3MgTWJjaGludXMGQ29ycG9y
:
5i5BozwFbvxCdM2INWzEaejdmejdCSDkgDGqgVtXXZnZeCtREOGME99nm3fHW7h
QkyXkg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID7TCCAtWgAWIBAgIBAJANBgkqhkiG9w0BAQUFADBIMQswCQYDVQQGEwJVUzE0
MDIGA1UEChMrSW50ZXJuYXRpb25hbCBCdXNpbmVzcyBhYWN0aW5lc3BDb3Jwb3Jh
:
:
i rUCKeSX1o3HGZFhMYw1KsYwog470qbYqDIqP+JM2N161GaNHi1DcW49qKvQTkV5
fg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDxDCCAqygAWIBAgIBADANBgkqhkiG9w0BAQUFADBIMQswCQYDVQQGEwJVUzE0
MDIGA1UEChMrSW50ZXJuYXRpb25hbCBCdXNpbmVzcyBhYWN0aW5lc3BDb3Jwb3Jh
:
:
bwnogYppATaH1z2PpMC3nqhyMv6B+NfAen1iMVbAFERrDRUuPD+Rt09s8ayEwVqp
3+HY0FBqh1I=
-----END CERTIFICATE-----

```

Figure 45. Illustration of required format for pasting into the GUI

Appendix C. Application Programming Interface (API) for monitoring products

IBM zAware provides an application programming interface (API) that system management products can use to request analytical data to display through their own graphic user interfaces. Through this API, system management products, such as IBM Tivoli OMEGAMON, can request and receive IBM zAware analytical data in XML format.

This data is equivalent to the information that is available through the **Analysis** page and **Interval view** in the IBM zAware GUI.

API versioning

Because the IBM zAware API might be modified to match changes to the functions provided through the IBM zAware GUI, each functional level of the API is identified by a version number. Each version number corresponds to a specific engineering change (EC) or microcode control level (MCL) for IBM zAware on the zEC12 or zBC12 central processor complex.

- To determine the EC and MCL levels installed on the zEC12 or zBC12 CPC on which the IBM zAware partition resides, use **System Information** under **Change Management** tasks on the Hardware Management Console (HMC). The EC number for the IBM zAware feature (SE-ZAWARE) is H09126.
- To determine the latest EC and MCL levels that are available from IBM, go to IBM Resource Link:
<http://www.ibm.com/servers/resourceLink>

Click **Tools** on the navigation panel. Then click **Machine information** under **Servers**, and enter your enterprise number, customer number, or machine serial number for the zEC12 or zBC12. You must register with IBM to search machine information.

To interoperate with multiple versions of the IBM zAware API, system management products that use the API must be designed to ignore, without error, the following possible modifications in XML responses:

- Any field that is not recognized by the application.
- Any header or body field that is not recognized by the application.

Table 58 lists each API version number, its corresponding MCL number, and a summary of modifications to the IBM zAware API for each version.

Table 58. Summary of API version updates for SE-ZAWARE MCLs

| API version | SE-ZAWARE MCL | Description |
|-------------|---------------|---|
| — | H09126.006 | Initial version of IBM zAware API. |
| 1 | H09126.021 | <ul style="list-style-type: none">• New XML fields returned for an LPAR request type.<ul style="list-style-type: none">– version– gmt_offset• New XML field returned for an INTERVAL request type: version |

Syntax and description of a GET request for IBM zAware data

Use an HTTP GET request to retrieve analytical data from IBM zAware for a specific monitored client in a specific sysplex. Depending on the request type, you can request the interval anomaly scores for one day or details for a specific 10-minute interval.

HTTP method and URI

GET `https://server_ip_address/zAware/authuser/Analysis?reqtype=request_type&time=time
&plexname=sysplex_name&lparname=system_name`

In this request:

- The URI variable `server_ip_address` is the IP address of the IBM zAware server.
- The remaining variables are parameters that are described in “Request contents.”

Example

The following example shows the syntax of a GET request from authorized user “admin12” for the analytical data available on 14 August 2011 for the z/OS monitored client named “z4”, which is a member of the sysplex named “ZPLEX2”.

GET `https://9.12.20.181/zAware/authuser/Analysis?reqtype=LPAR&time=20110814&lparname=z4&plexname=ZPLEX2`

Request contents

The following list describes the parameters in the GET request. All parameters are required, and can be specified in any order.

reqtype

Indicates what type of analytic data that you are requesting from the IBM zAware server.

LPAR

Requests analytical data for one day for one monitored client in a specific sysplex. The returned analytical data is equivalent to the information in the **Analysis** page display in the IBM zAware graphical user interface (GUI). The returned data provides interval anomaly scores for each interval since UTC midnight on the date indicated by the *time* variable. If *time* specifies the current date, the IBM zAware returns interval anomaly scores for every interval that has occurred. If *time* specifies a prior date, the IBM zAware returns interval anomaly scores for 144 intervals.

INTERVAL

Requests analytical data for a specific 10-minute time interval for one monitored client in a specific sysplex. The returned analytical data is equivalent to the information in the **Interval view** display in the IBM zAware GUI. The returned data provides details about each unique message ID that was issued during the 10-minute interval indicated by the *time* variable.

time

| Indicates the date and time period for which analytical data is requested, specified in the following
| format:
| `YYYYMMDDhhmm00`

| The *hhmm00* portion is required for an INTERVAL request, and optional for an LPAR request. If you
| specify the time period, use 24-hour clock time.

plexname

Specifies the name of the sysplex to which the monitored client belongs.

lparname

Specifies the name of the monitored client for which analytical data is requested.

Response contents

On successful completion, the response is an XML document that matches the request type:

- “XML for an LPAR request” on page 215 describes the returned XML for an LPAR request.
- “XML for an INTERVAL request” on page 218 describes the returned XML for an INTERVAL request.

Authorization requirements

Before you can send a GET request to retrieve analysis results, you must authenticate to the IBM zAware server with a user ID that is defined in the repository that your installation configured for user authentication to the IBM zAware server. The user ID must be assigned to either the User or the Administrator role through the **Administration > Configuration > Role Mapping** page in the IBM zAware GUI.

To authenticate to the IBM zAware server, issue a POST request to the server IP address:

POST `https://server_ip_address/zAware/j_security_check`

Through the following parameters, supply your user ID and password with your POST request:

`j_username=username`
`j_password=password`

Because authentication relies on the use of cookies, your user agent must be configured to accept, save, and send cookies.

HTTP status and reason codes

On successful completion, the HTTP status code 200 (OK) is returned and the response body is provided as described in “Response contents” on page 214. The following HTTP status codes can be returned for the indicated errors; the response body is a standard error response body providing an associated error message.

| HTTP error status code | Description |
|----------------------------------|--|
| 200 (OK) | The IBM zAware server returned XML data for the request. |
| 204 (No content) | The IBM zAware server did not return any XML data for the request. Check the parameter values that you supplied in the request. For an INTERVAL request, this error code is returned if interval data is not available for the specified interval on the specified date. |
| 400 (Bad Request) | The IBM zAware server did not return any XML data for the request. Check the parameter types that you supplied in the request. |
| 403 (Forbidden) | The IBM zAware server did not return any XML data for the request. Make sure that your program meets the authorization requirements in “Authorization requirements.” |
| 404 (Not Found) | No XML data was returned because the request specified a <code>server_ip_address</code> that is not a valid address for an IBM zAware server. |
| 503 (Server Environmental Error) | Storage devices are not configured for the IBM zAware server so no analytical data is available. |

XML for an LPAR request

This topic provides the XML structure, XML element descriptions, and a sample XML response that the IBM zAware server returns in response to an HTTP GET method with an LPAR request type. This XML response contains information that is equivalent to the interval anomaly scores that the server displays through the **Analysis** page in the IBM zAware graphical user interface (GUI).

The following code illustrates the XML structure of the response to an HTTP GET method with an LPAR request type. The major element is the **systems** element, which identifies the specific date and monitored client (system) for which analytical data was requested. The **systems** element also identifies the number and size of intervals returned in the XML document. The XML also contains one **interval** element for each 10-minute interval since UTC midnight on the requested date. The **interval** element provides the interval anomaly score and number of unique message IDs that were issued during the specific interval.

“XML element descriptions for an LPAR request” provides additional information about each element in the XML response.

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.example.org/MelodyCorePlex" xmlns="http://www.example.org/MelodyCorePlex"
  elementFormDefault="qualified">

  <xs:element name="systems" >
    <xs:complexType>
      <xs:sequence>
|      <xs:element name="version" type="xs:int" />
|      <xs:element name="start_time" type="xs:dateTime" />
|      <xs:element name="end_time" type="xs:dateTime" />
|      <xs:element name="gmt_offset" type="xs:string" />
|      <xs:element name="number_intervals" type="xs:int" />
|      <xs:element name="interval_size" type="xs:int" />
|      <xs:element name="system" type="systems_system_type"
|        maxOccurs="unbounded" />
|      </xs:sequence>
|    </xs:complexType>
|  </xs:element>

  <xs:complexType name="systems_system_type">
    <xs:sequence>
|      <xs:element name="interval" type="systems_interval_type"
|        minOccurs="0" maxOccurs="unbounded" />
|    </xs:sequence>
|    <xs:attribute name="sys_id" type="xs:string" use="required" />
|  </xs:complexType>

  <xs:complexType name="systems_interval_type">
    <xs:sequence>
|      <xs:element name="num_unique_msg_ids" type="xs:int" />
|      <xs:element name="anomaly_score" type="xs:double" />
|    </xs:sequence>
|  </xs:complexType>

</xs:schema>
```

XML element descriptions for an LPAR request

The following list describes the major elements in the **systems** element.

| **version**

- | An integer that identifies the version of the IBM zAware application programming interface (API).
- | For information about specific API versions, see “API versioning” on page 213.

start_time

Indicates the beginning of the first interval for which data is available for the specified system on the date in the LPAR request. The start time is indicated in the XML dateTime data type format in Coordinated Universal Time (UTC).

YYYY-MM-DDThh:mm:ss.tttZ

end_time

Indicates the beginning of the first interval *after* the date specified in the LPAR request. The end time is indicated in the XML dateTime data type format in Coordinated Universal Time (UTC).

YYYY-MM-DDThh:mm:ss.tttZ

| **gmt_offset**

- | An integer that indicates the difference in hours and minutes from Coordinated Universal Time (UTC) for the requested start time.

number_intervals

An integer that indicates the number of 10-minute intervals for which analytical data is available for

the system and the date specified on the LPAR request. Analytical data might not be available this system for all intervals during the date specified on the request. Data is not available under the following circumstances:

- The monitored client was not connected and sending current data to the IBM zAware server on the specified date.
- The monitored client was added to the sysplex topology after the specified date.

Note that analytical data is not available for the dates for which you supplied priming data, unless the monitored client was connected and sending data to the IBM zAware server on those dates. The server uses priming data only for creating the model of system behavior.

interval_size

An integer that indicates the number of seconds in an interval.

system

An element that provides additional details about intervals for the system specified on the LPAR request. The `sys_id` attribute for this element provides the name of the system that was specified on the LPAR request, and the name of the sysplex to which the system belongs.

interval

An element that provides additional details about a specific 10-minute interval. The XML response contains one interval element for each element for which analytical data is available for the system and the date specified on the LPAR request.

num_unique_msg_ids

An integer that provides the number of unique message IDs that were issued during this 10-minute interval. If the same message ID was issued more than once during the interval, the message ID is counted only once.

anomaly_score

A double value that provides the anomaly score for this interval. The interval anomaly score is the percentile of the sum of each anomaly score for individual message IDs within an interval. When the IBM zAware server uses priming data and current data to create a model of system behavior, a process that is called “training”, the server captures the distribution of interval anomaly scores for all intervals that are represented in the training data. The server uses the distribution results and uses them to establish the range of values for each percentile.

The possible interval anomaly scores are:

0 through 99.4

The interval contains messages and message clusters that match or exhibit relatively insignificant differences in expected behavior, as defined in the IBM zAware model. A score of 0 is possible because the server eliminates all expected, in-context messages from its scoring calculation. A score of 0 indicates intervals that exhibit no difference in behavior compared to the system model. In the bar graph display, these intervals are colored with the lightest blue shade.

Intervals with scores that are greater than 0 but less than 99.5 contain some messages that are unexpected or issued out of context. Scores in this range indicate intervals that do not vary significantly from the system model. In the bar graph display, these intervals are colored with varying shades of blue.

99.5 Intervals with this score contain some rarely seen, unexpected, or out-of-context messages. Generally speaking, this score indicates intervals with some differences from the system model but do not contain messages of much diagnostic value. In the bar graph display, these intervals are colored with the darkest blue shade.

99.6 - 100

Intervals with this score contain rarely seen messages (these messages appear in the model only once or twice), or many messages that are unexpected or issued out of

context. This score indicates intervals with more differences from the system model; these intervals can contain messages that might help you diagnose anomalous system behavior. In the bar graph display, these intervals are the color gold.

- 101 Intervals with this score exhibit the most significant differences from the system model; these intervals contain messages that merit investigation. In the bar graph display, these intervals are the color orange. IBM zAware assigns this score to intervals that contain:
- Unique message IDs that the server has not detected previously in the client model
 - Unusual or unexpected messages
 - Messages that IBM rules define as critical
 - A much higher volume of messages than expected

Sample XML response for an LPAR request

This sample provides the returned XML in response to a GET request for the interval anomaly scores for a system named "C05" in sysplex "ABCPLEX" on 12 September 2012. The sample response shown is formatted for publication and contains information for only a few of the 144 returned intervals.

GET method:

GET https://9.xx.xx.xxx/zAware/authuser/Analysis?reqtype=LPAR&time=20120912&lparname=C05&plexname=ABCPLEX

XML response:

```
<?xml version='1.0' encoding='UTF-8' ?>
<?xml-stylesheet href='./xslt/MelodyCorePlex.xsl' type='text/xsl' ?>
<systems xsi:noNamespaceSchemaLocation="xslt/MelodyCorePlex.xsd"
xmlns="http://www.example.org/MelodyCorePlex" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<start_time>2012-09-12T00:00:00.000Z</start_time>
<end_time>2012-09-13T00:00:00.000Z</end_time>
<number_intervals>144</number_intervals>
<interval_size>600</interval_size>
<system sys_id="ABCPLEX-C05">
  <interval>
    <num_unique_msg_ids>71</num_unique_msg_ids>
    <anomaly_score>82.0</anomaly_score>
  </interval>
  <interval>
    <num_unique_msg_ids>51</num_unique_msg_ids>
    <anomaly_score>52.0</anomaly_score>
  </interval>
  :
  <interval>
    <num_unique_msg_ids>99</num_unique_msg_ids>
    <anomaly_score>98.7</anomaly_score>
  </interval>
  <interval>
    <num_unique_msg_ids>0</num_unique_msg_ids>
    <anomaly_score>0.0</anomaly_score>
  </interval>
</system>
</systems>
```

XML for an INTERVAL request

This topic provides the XML structure, XML element descriptions, and a sample XML response that the IBM zAware server returns in response to an HTTP GET method with an INTERVAL request type. This XML response contains information that is equivalent to the interval and message details that the server displays through the **Interval view** in the IBM zAware graphical user interface (GUI).

The following code illustrates the XML structure of the response to an HTTP GET method with an INTERVAL request type. The major element is the **interval** element, which contains information about a specific 10-minute interval for a specific system that is established as an IBM zAware monitored client. The **interval** element also contains one **interval_message** element for each unique message issued during the interval. If the same message ID was issued more than once during the selected interval, the XML contains only one **interval_message** element for that unique message ID.

“XML element descriptions for an INTERVAL request” on page 220 provides additional information about each element in the XML response.

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.example.org/MelodyCoreInterval"
  xmlns="http://www.example.org/MelodyCoreInterval"
  elementFormDefault="qualified">

  <xs:element name="interval">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="version" type="xs:int" />
        <xs:element name="sys_id" type="xs:string"/>
        <xs:element name="start_time" type="xs:dateTime" />
        <xs:element name="end_time" type="xs:dateTime" />
        <xs:element name="anomaly_score" type="xs:double"/>
        <xs:element name="model_internal_id" type="xs:int"/>
        <xs:element name="melody_version" type="xs:int"/>
        <xs:element name="interval_message" type="interval_message_type"
          maxOccurs="unbounded" minOccurs="0"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="interval_message_type">
    <xs:sequence>
      <xs:element name="num_instances" type="xs:int"/>
      <xs:element name="bernoulli" type="xs:double"/>
      <xs:element name="cluster_id" type="xs:int"/>
      <xs:element name="poisson" type="xs:double"/>
      <xs:element name="intCont" type="xs:double"/>
      <xs:element name="normIntCont" type="xs:double"/>
      <xs:element name="anomaly" type="xs:double"/>
      <xs:element name="cluster_status" type="xs:string"/>
      <xs:element name="critical_words" type="xs:double"/>
      <xs:element name="text_sum" type="xs:string"/>
      <xs:element name="text_smp" type="xs:string"/>
      <xs:element name="time_vec" type="interval_time_vector_type"/>
      <xs:element name="active_rules" type="active_rules_type" maxOccurs="1" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="msg_id" type="xs:string" use="required" />
  </xs:complexType>

  <xs:complexType name="interval_time_vector_type">
    <xs:sequence>
      <xs:element name="occ" maxOccurs="unbounded" minOccurs="0" type="xs:int"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="active_rules_type">
    <xs:sequence>
      <xs:element name="rule" type="rule_type" maxOccurs="unbounded" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="rule_type">
    <xs:sequence>
      <xs:element name="name" type="xs:string" />
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="rule_type">
    <xs:sequence>
      <xs:element name="name" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
```

```

        <xs:element name="action" type="xs:string" />
    </xs:sequence>
</xs:complexType>
</xs:schema>

```

XML element descriptions for an INTERVAL request

The following list describes the major elements in the **interval** element.

version

- | An integer that identifies the version of the IBM zAware application programming interface (API).
- | For information about specific API versions, see “API versioning” on page 213.

sys_id

A string that provides the name of the system that was specified on the INTERVAL request, and the name of the sysplex to which the system belongs.

start_time

Indicates the beginning of the first interval for which data is available for the specified system on the date in the LPAR request. The start time is indicated in the XML dateTime data type format in Coordinated Universal Time (UTC).

YYYY-MM-DDThh:mm:ss.tttZ

end_time

Indicates the beginning of the first interval *after* the date specified in the LPAR request. The end time is indicated in the XML dateTime data type format in Coordinated Universal Time (UTC).

YYYY-MM-DDThh:mm:ss.tttZ

anomaly_score

A double value that provides the anomaly score for this interval. The interval anomaly score is the percentile of the sum of each anomaly score for individual message IDs within an interval. When the IBM zAware server uses priming data and current data to create a model of system behavior, a process that is called “training”, the server captures the distribution of interval anomaly scores for all intervals that are represented in the training data. The server uses the distribution results and uses them to establish the range of values for each percentile.

The possible interval anomaly scores are:

0 through 99.4

The interval contains messages and message clusters that match or exhibit relatively insignificant differences in expected behavior, as defined in the IBM zAware model. A score of 0 is possible because the server eliminates all expected, in-context messages from its scoring calculation. A score of 0 indicates intervals that exhibit no difference in behavior compared to the system model. In the bar graph display, these intervals are colored with the lightest blue shade.

Intervals with scores that are greater than 0 but less than 99.5 contain some messages that are unexpected or issued out of context. Scores in this range indicate intervals that do not vary significantly from the system model. In the bar graph display, these intervals are colored with varying shades of blue.

- 99.5** Intervals with this score contain some rarely seen, unexpected, or out-of-context messages. Generally speaking, this score indicates intervals with some differences from the system model but do not contain messages of much diagnostic value. In the bar graph display, these intervals are colored with the darkest blue shade.

99.6 - 100

Intervals with this score contain rarely seen messages (these messages appear in the model only once or twice), or many messages that are unexpected or issued out of context. This

score indicates intervals with more differences from the system model; these intervals can contain messages that might help you diagnose anomalous system behavior. In the bar graph display, these intervals are the color gold.

101 Intervals with this score exhibit the most significant differences from the system model; these intervals contain messages that merit investigation. In the bar graph display, these intervals are the color orange. IBM zAware assigns this score to intervals that contain:

- Unique message IDs that the server has not detected previously in the client model
- Unusual or unexpected messages
- Messages that IBM rules define as critical
- A much higher volume of messages than expected

model_internal_id

An integer that the IBM zAware server uses to identify this system model.

melody_version

An integer that represents the version of the analytics engine that the IBM zAware server is using.

interval_message

The XML response contains one **interval_message** element for each unique message ID that was issued within the interval specified on the LPAR request. The attribute `msg_id` on each **interval_message** element contains a string that identifies the unique message ID.

Each **interval_message** contains the following attributes for the message.

num_instances

An integer that specifies the number of times that this message was issued within this 10-minute interval.

bernoulli

A double value that indicates how frequently the message ID is issued within a sampled set of 10-minute intervals in the system model. Values range from 1 to 101:

- A value of 1 indicates that the message is issued in almost all intervals in the model.
- A value of 100 indicates that the message is issued in almost none of the intervals in the model.
- A value of 101 indicates that this message ID has not been issued in any interval in the model.

cluster_id

An integer that represents the identifier of the cluster to which this message belongs. When the message is not part of a recognized cluster, the cluster ID is -1.

poisson

A double value that indicates how closely the message ID distribution in current data matches the Poisson distribution of that message ID in data during the training period for the system model. This value is provided only for message IDs that are not part of a cluster. The higher the **poisson** value, the greater the difference from expected behavior.

intCont

A double value that indicates the relative contribution of this message to the interval anomaly score for the 10-minute interval. This interval score is a function of the message anomaly score, the number of times that the message appears within this interval, and whether the message appeared in context.

anomaly

A double value that indicates the rarity of this specific message ID within the selected interval. The anomaly score is a combination of the interval contribution score for this message and the rule, if any, that is in effect for this message. Higher scores indicate greater anomaly so messages with high anomaly scores are more likely to indicate a problem.

cluster_status

A string that indicates whether or not this message is part of an expected pattern of messages associated with a routine system event (for example, starting a subsystem or workload). IBM

zAware identifies and recognizes these patterns or groups, which are called “clusters”, and the specific message IDs that constitute a specific cluster. When analyzing data from a monitored client, the server determines whether a specific message is expected to be issued within a specific cluster. A message that is issued out of context (without the other messages in the same cluster) might indicate a problem.

Values for **cluster_status** are:

New IBM zAware has not previously detected this message in the client model.

Unclustered

This message is not part of a defined cluster.

In context

This message was issued as expected, within a cluster to which this message belongs.

Out of context

This message is expected to be issued as part of a specific cluster but was issued in a different context.

critical_words

A double value that indicates whether the message contains specific words that indicate potential problems. Critical words include “abend”, “failure”, and “warning”.

text_sum

A string that contains a summary of the common message text that was issued for each occurrence of the same message.

text_smp

A string that contains the full message text for the first occurrence of this message within the interval.

time_vec

The XML response contains one **time_vec** element for each unique message ID that was issued within the interval specified on the LPAR request.

occ

The XML response contains one **occ** element for each time that this message ID was issued within the interval specified on the LPAR request.

active_rules

The XML response contains one **active_rules** element for each unique message ID that was issued within the interval specified on the LPAR request.

rule

The XML response contains one **rule** element for each rule that is in effect for this message ID.

name

A string that contains the name of the rule that was applied for this message. The rule can be one of the following types:

- Predefined by IBM.
- Assigned by IBM zAware as a result of the analysis of training data.
- Assigned by IBM zAware when an administrator has identified the message as one that IBM zAware is to ignore during analysis, either until the next model is built or until an administrator manually resets the ignore status.

action

A string that contains the status value associated with the applied rule. Possible values are:

CRITICAL

An IBM rule identifies this message as critical for diagnosing a potential system problem. For example, message IXC101I, which indicates that a system is being removed from a sysplex, is classified as critical.

IMPORTANT

An IBM rule identifies this message as likely to indicate a problem. For example, message IEA911E, which indicates that an SVC dump has been taken, is classified as important.

INTERESTING

An IBM rule identifies this message as indicative of a diagnostically useful event, such as a health check exception.

NONE

No rule is applied for this message.

NON-INTERESTING

One of the following conditions is true for this message:

- A predefined IBM rule or an IBM zAware-assigned rule identifies this message as one with little or no diagnostic value.
- An administrator has identified the message as one that IBM zAware is to ignore during analysis, either until the next model is built or until an administrator manually resets the ignore status.

Sample XML response for an INTERVAL request

This sample provides the returned XML in response to a GET request for the details for a system named “CB8E” in sysplex “ABCPLEX” during the 10-minute interval that started on 12 September 2012 at 14:20:00 UTC. The sample response shown is formatted for publication and contains information for only a few of the returned messages issued within this interval.

GET method:

```
GET https://9.xx.xx.xx/zAware/authuser/Analysis?reqtype=INTERVAL&intervalid=86
&time=20120912&lpname=CB8E&plexname=ABCPLEX
```

XML response:

```
<?xml version='1.0' encoding='UTF-8' ?>
<?xml-stylesheet href='./xslt/MelodyCoreInterval.xsl' type='text/xsl' ?>
<interval xsi:noNamespaceSchemaLocation="xslt/MelodyCoreInterval.xsd"
  xmlns="http://www.example.org/MelodyCoreInterval"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <sys_id>ABCPLEX-CB8E</sys_id>
  <start_time>2012-09-12T14:20:00.000Z</start_time>
  <end_time>2012-09-12T14:30:00.000Z</end_time>
  <anomaly_score>95.3</anomaly_score>
  <model_internal_id>2</model_internal_id>
  <melody_version>170</melody_version>
  <interval_message msg_id="BLWH0001E">
    <num_instances>1</num_instances>
    <bernoulli>58.0</bernoulli>
    <cluster_id>120</cluster_id>
    <poisson>0.0</poisson>
    <intCont>0.0</intCont>
    <normIntCont>0.0</normIntCont>
    <anomaly>0.0</anomaly>
    <cluster_status>IN_CONTEXT</cluster_status>
    <critical_words>0.0</critical_words>
    <text_sum>AutoIPL policy is not active.</text_sum>
    <text_smp>AutoIPL policy is not active.</text_smp>
    <time_vec>
      <occ>0</occ>
    </time_vec>
  </interval_message>
  <interval_message msg_id="HZS0002E">
    <num_instances>12</num_instances>
    <bernoulli>12.0</bernoulli>
```

```

<cluster_id>-1</cluster_id>
<poisson>3.245</poisson>
<intCont>3.245</intCont>
<normIntCont>8.947</normIntCont>
<anomaly>0.96</anomaly>
<cluster_status>UNCLUSTERED</cluster_status>
<critical_words>0.0</critical_words>
<text_sum>CHECK(*,*):</text_sum>
<text_smp>CHECK(IBMSVA,SVA_AUTOIPL_DEFINED):</text_smp>
<time_vec>
  <occ>0</occ>
  <occ>1</occ>
  <occ>4</occ>
  <occ>16</occ>
  <occ>24</occ>
  <occ>25</occ>
</time_vec>
</interval_message>

:
</interval>

```

Appendix D. IBM zAware operational messages

This topic provides revised message text and descriptions of the operational messages that the IBM zAware server issues. The revised message text matches the text used in engineering change (EC) and microcode control level (MCL) H09126.024, and later levels. Use the **Notifications** page in the IBM zAware graphical user interface (GUI) to view and manage these messages. User IDs assigned to either the Administrator or User role can view the **Notifications** page but only an administrator can remove a message from the display on the page.

AIFB0001E IBM zAware encountered an internal error with reason code *code*. Search problem reporting databases for a fix for this error. If no fix exists, report this message ID and reason code to IBM Support.

Explanation: IBM zAware encountered an internal error indicated by reason code *code*.

System action: For most internal errors, Licensed Internal Code automatically gathers and sends diagnostic information to IBM if the “Call Home” feature is enabled on the IBM zAware host system.

Response: On the Hardware Management Console (HMC) for the IBM zAware host system, check for outstanding hardware messages that indicate a “Call Home” call associated with the IBM zAware partition. If a service call has not been sent automatically, search problem reporting databases for a fix for this error. If no fix exists, request IBM support by generating a Type V Viewable PMH (PMV) record to report this message ID and reason code.

For additional information, see Chapter 24, “Reporting IBM zAware problems to IBM,” on page 199. If you do not have a maintenance contract with IBM, use the questions at the end of that topic to collect the information that you might need to report the problem to your hardware maintenance provider.

AIFB0003I IBM zAware successfully assigned priming data from system *system_name* to sysplex *sysplex_name*.

Explanation: Through the **Priming Data** tab of the IBM zAware graphical user interface (GUI), an administrator submitted a request to assign priming data for the monitored client identified by *system_name* to the sysplex *sysplex_name*. IBM zAware successfully completed the assignment request.

System action: IBM zAware recycles the analytics engine so that your changes take effect. IBM zAware is ready to use this priming data to build a model of behavior for the monitored client that is uniquely identified by its sysplex and system name.

Response: None required. To build a model for this system:

1. Navigate to the Training Sets page and select the system.
2. From the Actions list, select **Request Training** to submit a request to build a model of system behavior.

AIFB0004I While attempting to assign priming data from system *system_name* to sysplex *sysplex_name*, IBM zAware encountered an error with reason code *code*. Search problem reporting databases for a fix for this error. If no fix exists, report this message ID and reason code to IBM Support.

Explanation: Through the **Priming Data** tab of the IBM zAware graphical user interface (GUI), an administrator submitted a request to assign priming data for the monitored client identified by *system_name* to the sysplex *sysplex_name*. IBM zAware could not successfully complete the request because it encountered an error indicated by the reason code *code*.

System action: On the **Priming Data** tab of the IBM zAware GUI, the system remains in the **Priming data by systems** list. IBM zAware retains the priming data for this system but cannot use it to build a model.

Response: Search problem reporting databases for a fix for this error. If no fix exists, request IBM support by generating a Type V Viewable PMH (PMV) record to report this message ID and reason code.

For additional information, see Chapter 24, “Reporting IBM zAware problems to IBM,” on page 199. If you do not have a maintenance contract with IBM, use the questions at the end of that topic to collect the information that you might need to report the problem to your hardware maintenance provider.

AIFB0005I IBM zAware successfully modified the system topology by moving system *system_name* from sysplex *source_sysplex_name* to sysplex *target_sysplex_name*.

Explanation: Through the **Sysplex Topology** tab of the IBM zAware graphical user interface (GUI), an administrator submitted a request to move the monitored client identified by *system_name* from the sysplex of which it is currently a member (*source_sysplex_name*) to a different sysplex in the topology (*target_sysplex_name*). IBM zAware successfully completed the request.

System action: IBM zAware recycles the analytics engine so that your changes take effect. When the **Sysplex Topology** tab is refreshed, the system is listed under the target sysplex (*target_sysplex_name*).

Response: None required.

AIFB0006I While attempting to move system *system_name* from sysplex *source_sysplex_name* to sysplex *target_sysplex_name*, IBM zAware encountered an error with reason code *code*. Search problem reporting databases for a fix for this error. If no fix exists, report this message ID and reason code to IBM Support.

Explanation: Through the **Sysplex Topology** tab of the IBM zAware graphical user interface (GUI), an administrator submitted a request to move the monitored client identified by *system_name* from the sysplex of which it is currently a member (*source_sysplex_name*) to a different sysplex in the topology (*target_sysplex_name*). IBM zAware could not successfully complete the request because it encountered an error indicated by the reason code *code*.

System action: In the **Sysplex Topology** tab of the IBM zAware GUI, the system remains listed under the source sysplex (*source_sysplex_name*).

Response: Search problem reporting databases for a fix for this error. If no fix exists, request IBM support by generating a Type V Viewable PMH (PMV) record to report this message ID and reason code.

For additional information, see Chapter 24, “Reporting IBM zAware problems to IBM,” on page 199. If you do not have a maintenance contract with IBM, use the questions at the end of that topic to collect the information that you might need to report the problem to your hardware maintenance provider.

AIFG0001E IBM zAware encountered an internal error. Search problem reporting databases for a fix for this error. If no fix exists, report this message ID to IBM Support.

Explanation: IBM zAware encountered an internal error.

System action: For most internal errors, Licensed Internal Code automatically gathers and sends diagnostic information to IBM if the “Call Home”

feature is enabled on the IBM zAware host system.

Response: On the Hardware Management Console (HMC) for the IBM zAware host system, check for outstanding hardware messages that indicate a “Call Home” call associated with the IBM zAware partition. If a service call has not been sent automatically, search problem reporting databases for a fix for this error. If no fix exists, request IBM support by generating a Type V Viewable PMH (PMV) record to report this message ID.

For additional information, see Chapter 24, “Reporting IBM zAware problems to IBM,” on page 199. If you do not have a maintenance contract with IBM, use the questions at the end of that topic to collect the information that you might need to report the problem to your hardware maintenance provider.

AIFP0001E IBM zAware encountered an internal error with reason code *code*. Search problem reporting databases for a fix for this error. If no fix exists, report this message ID and reason code to IBM Support.

Explanation: IBM zAware encountered an internal error indicated by reason code *code*.

System action: For most internal errors, Licensed Internal Code automatically gathers and sends diagnostic information to IBM if the “Call Home” feature is enabled on the IBM zAware host system.

Response: On the Hardware Management Console (HMC) for the IBM zAware host system, check for outstanding hardware messages that indicate a “Call Home” call associated with the IBM zAware partition. If a service call has not been sent automatically, search problem reporting databases for a fix for this error. If no fix exists, request IBM support by generating a Type V Viewable PMH (PMV) record to report this message ID and reason code.

For additional information, see Chapter 24, “Reporting IBM zAware problems to IBM,” on page 199. If you do not have a maintenance contract with IBM, use the questions at the end of that topic to collect the information that you might need to report the problem to your hardware maintenance provider.

AIFP0002E IBM zAware could not initialize the physical volume *device_id* because of a disk or I/O error. If necessary, go to the Data Storage page in the IBM zAware GUI to select another device to add.

Explanation: Through the IBM zAware graphical user interface (GUI), an administrator used the **Add and Remove Devices** function on the Data Storage page to add one or more devices to the IBM zAware storage configuration. IBM zAware could not add the device

identified by *device_id* because of a disk or input/output (I/O) error.

System action: IBM zAware does not add *device_id* to the list of in-use devices. If the add request included multiple storage devices, some of which remain to be processed, IBM zAware continues to process the request for those devices.

Response: On the Support Element (SE) for the IBM zAware host system, check for hardware messages that indicate I/O or other problems related to this storage device. If possible, correct the error and retry the add request. Otherwise, select another device to add to the IBM zAware storage configuration.

AIFP0003I IBM zAware started processing a request to add storage device *device_id*.

Explanation: Through the IBM zAware graphical user interface (GUI), an administrator used the **Add and Remove Devices** function on the Data Storage page to add one or more devices to the IBM zAware storage configuration. This message indicates that IBM zAware has started to process the request to add the storage device identified by *device_id*.

System action: IBM zAware continues to process the add request, and issues message AIFP0004I after successfully adding the device.

Response: None.

AIFP0004I IBM zAware successfully added storage device *device_id*.

Explanation: Through the IBM zAware graphical user interface (GUI), an administrator used the **Add and Remove Devices** function on the Data Storage page to add one or more devices to the IBM zAware storage configuration. This message indicates that IBM zAware successfully processed the request to add the storage device identified by *device_id*.

System action: IBM zAware uses the device for processing and storage of analysis results. If the add request included multiple storage devices, some of which remain to be processed, IBM zAware continues to process the request for those remaining devices.

Response: None.

AIFP0005I IBM zAware rejected a request to add or remove a storage device because another storage operation is in progress. When the operation completes, retry the request.

Explanation: Through the IBM zAware graphical user interface (GUI), an administrator used the **Add and Remove Devices** function on the Data Storage page to add or remove one or more devices. IBM zAware could not process this request because a prior request to add or remove storage devices is still in progress.

System action: IBM zAware continues to process the prior request.

Response: Resubmit the request after IBM zAware completes processing the prior request.

AIFP0006E IBM zAware detected that at least one in-use persistent storage device, *device_id*, is missing. Try reattaching the device identified by *device_id* and reactivating the IBM zAware partition. See the AIFP0013E message description to determine whether additional corrective actions are necessary.

Explanation: IBM zAware detected that an in-use persistent storage device, identified by *device_id*, is no longer attached to the IBM zAware partition. It might have been removed or disconnected through storage operations that are not provided through the Data Storage page of the IBM zAware GUI, such as:

- Replacing the I/O definition file (IODF) for the host system with an IODF that does not contain the in-use storage devices for IBM zAware.
- Using the Support Element (SE) to take offline one or more channel paths (CHPIDs) for storage devices or for the network through which those devices are connected to the IBM zAware partition.

Additional in-use storage devices also might be missing, as indicated by message “AIFP0013E” on page 230.

System action: When an in-use storage device becomes unavailable, IBM zAware operations stop. To a user of the IBM zAware GUI, the GUI appears to hang. On the SE for the IBM zAware host system, hardware messages indicate input/output (I/O) problems related to the loss of access to physical storage devices.

Response: If possible, try to reattach the device identified by *device_id* and reactivate the IBM zAware partition.

If you cannot reattach the device, see the “AIFP0013E” on page 230 message description for additional information and instructions for correcting the IBM zAware storage configuration.

AIFP0007I During activation, IBM zAware was not able to reconnect to the previously configured LDAP server *hostname:port*. Only the master user ID and locally defined users are able to log in to the GUI until the LDAP server is available and an administrator reconnects IBM zAware to it by reapplying the LDAP configuration through the LDAP Settings page.

Explanation: When the IBM zAware partition is reactivated at any time after its initial configuration,

IBM zAware attempts to reconnect to the previously configured Lightweight Directory Access Protocol (LDAP) server. This reconnection attempt fails if the LDAP server is not available or the LDAP configuration has changed. The previously configured LDAP server is identified by *hostname* and the port number (*port*) used for communication between the LDAP and IBM zAware servers. Without access to the LDAP repository, you can successfully log in to the IBM zAware graphical user interface (GUI) using the master user ID and password, which are specified through the activation profile for the IBM zAware partition. If you have set up a local file-based repository of user IDs, you can use one of those locally defined IDs only if you previously assigned an IBM zAware “Administrator” role for them through the Role Mapping page in the GUI.

System action: Activation of IBM zAware continues.

Response: To log in to the IBM zAware GUI after activation completes, you must use either the master user ID, or a locally defined user ID that previously was mapped to an “Administrator” role.

To enable access for users that are defined in the LDAP server:

1. Determine why the LDAP server was not accessible and correct the problem.
2. Through the IBM zAware, click the **LDAP Settings** tab on the Security page and verify the values shown for the general and group LDAP settings. Click **Apply** to reconnect IBM zAware to the LDAP server.

AIFP0008I IBM zAware was unable to remove storage device *device_id*. Report this message ID to IBM Support.

Explanation: Through the IBM zAware graphical user interface (GUI), an administrator used the **Add and Remove Devices** function on the Data Storage page to remove one or more devices to the IBM zAware storage configuration. IBM zAware encountered an internal error while processing the request to remove the storage device identified by the variable *device_id*.

System action: IBM zAware does not remove *device_id* from the list of in-use devices. If the remove request included multiple storage devices, some of which remain to be processed, IBM zAware continues to process the request for those devices.

Response: On the Hardware Management Console (HMC) for the IBM zAware host system, check for outstanding hardware messages that indicate a “Call Home” call associated with the IBM zAware partition. If a service call has not been sent automatically, request IBM support by generating a Type V Viewable PMH (PMV) record to report this message ID and reason code.

For additional information, see Chapter 24, “Reporting

IBM zAware problems to IBM,” on page 199. If you do not have a maintenance contract with IBM, use the questions at the end of that topic to collect the information that you might need to report the problem to your hardware maintenance provider.

AIFP0009I IBM zAware started processing a request to remove storage device *device_id* from the set of in-use devices.

Explanation: Through the IBM zAware graphical user interface (GUI), an administrator used the **Add and Remove Devices** function on the Data Storage page to remove one or more devices to the IBM zAware storage configuration. This message indicates that IBM zAware has started to process the request to remove the storage device identified by *device_id*.

System action: IBM zAware continues to process the remove request. IBM zAware issues message AIFP0010I when it has successfully removed the device. If it cannot remove the device at this time, IBM zAware places the device in “Pending Removal” status.

Response: Go to the **Data Storage** tab in the IBM zAware GUI to check the current status of the device. Because IBM zAware processes storage requests asynchronously, you need to click **Refresh** at least once to display the current status of the device in the **Data Storage Devices** table. When IBM zAware is processing a remove request, the device status is “Being Removed”; when the process completes, the status is either “Available” or “Pending Removal”. If IBM zAware placed the device in “Pending Removal” status, click **Apply Pending Removals** on the **Data Storage** tab to remove the device.

AIFP0010I IBM zAware successfully removed storage device *device_id* from the set of in-use devices.

Explanation: Through the IBM zAware graphical user interface (GUI), an administrator used the **Add and Remove Devices** function on the Data Storage page to remove one or more devices to the IBM zAware storage configuration. This message indicates that IBM zAware successfully processed the request to remove the storage device identified by *device_id*.

System action: IBM zAware moves data from *device_id* to the remaining in-use storage devices, and no longer uses *device_id* for processing and storage of analysis results. If the remove request included multiple storage devices, some of which remain to be processed, IBM zAware continues to process the request for those remaining devices.

Response: None required. At this point, a storage administrator can detach *device_id* from the IBM zAware partition without disrupting IBM zAware operations.

AIFP0011E During activation, IBM zAware encountered an internal error while attempting to reconnect to the previously configured LDAP server *hostname:port*. This error might have initiated a call home to IBM Support. Only the master user ID and locally defined users are able to log in to the GUI until the LDAP server is available and an administrator reconnects IBM zAware to it by reapplying the LDAP configuration through the LDAP Settings page.

Explanation: When the IBM zAware partition is reactivated at any time after its initial configuration, IBM zAware attempts to reconnect to the previously configured Lightweight Directory Access Protocol (LDAP) server. During a reconnection attempt, IBM zAware encountered an internal error. The previously configured LDAP server is identified by *hostname* and the port number (*port*) used for communication between the LDAP and IBM zAware servers. Without access to the LDAP repository, you can successfully log in to the IBM zAware graphical user interface (GUI) using the master user ID and password, which are specified through the activation profile for the IBM zAware partition. If you have set up a local file-based repository of user IDs, you can use one of those locally defined IDs only if you previously assigned an IBM zAware “Administrator” role for them through the Role Mapping page in the GUI.

System action: Activation of IBM zAware continues. This internal error might have resulted in a “Call Home” service call; in this case, Licensed Internal Code automatically gathers and sends diagnostic information to IBM if the “Call Home” feature is enabled on the IBM zAware host system.

Response: To log in to the IBM zAware GUI after activation completes, you must use either the master user ID, or a locally defined user ID that previously was mapped to an “Administrator” role. Through the IBM zAware, click the **LDAP Settings** tab on the Security page and verify the values shown for the general and group LDAP settings. Click **Apply** to reconnect IBM zAware to the LDAP server.

If the problem persists:

- On the Hardware Management Console (HMC) for the IBM zAware host system, check for outstanding hardware messages that indicate a “Call Home” call associated with the IBM zAware partition. If a service call has not been sent automatically, search problem reporting databases for a fix for this error.
- If no fix exists, request IBM support by generating a Type V Viewable PMH (PMV) record to report this message ID.

For additional information, see Chapter 24, “Reporting IBM zAware problems to IBM,” on page 199. If you do

not have a maintenance contract with IBM, use the questions at the end of that topic to collect the information that you might need to report the problem to your hardware maintenance provider.

AIFP0012I Persistent storage device *device_id* was configured and in use by IBM zAware, but is no longer required and has been removed from the list of in-use storage devices.

Explanation: When your installation configures a primary IBM zAware partition and an alternate IBM zAware partition for switchover situations, only one IBM zAware server can be active at a given time but both servers must have access to the same data. To correctly configure persistent storage for primary and alternate IBM zAware partitions, your installation must define physically separate but equivalent sets of storage devices for each partition, and also set up replication to copy the content of the primary storage devices to the alternate storage devices. For data replication to be successful, the number of storage devices in the primary set must match the number of devices in the alternate set. Additionally, each alternate device must be equivalent in size to the primary device.

Message AIFP0012I is issued when the currently active IBM zAware server takes corrective action to resolve a mismatch that results from the removal of a device from either the primary or the alternate set of storage devices. Consider the following example, for which a storage administrator has defined two sets of 3390 DASD for IBM zAware:

- Devices 3001 through 3005 are intended for the exclusive use of the primary server of IBM zAware.
- Equivalent devices 9111 through 9115 are intended for the exclusive use of the alternate server.
- Through the IBM zAware graphical user interface (GUI), the administrator initially configures the primary server to use only devices 3002 and 3004.
- Through other tools or interfaces, the administrator also sets up replication such that the content of device 3002 is periodically copied to device 9112, and the content of device 3004 is copied to device 9114. For successful replication, device 9112 must be the same size as device 3002; similarly, device 9114 must be equivalent to device 3004.
- To successfully use the alternate server of IBM zAware when the primary server is no longer available, an administrator must use the GUI to initially configure the alternate server to use both devices 9112 and 9114, the devices that contain the data copied from their equivalent primary in-use devices. To configure the alternate server, the administrator:
 1. Deactivates the primary partition of IBM zAware, and activates the alternate partition.

2. Uses the IBM zAware GUI to add devices 9112 and 9114 to the storage configuration for the alternate server.
3. Deactivates the alternate partition of IBM zAware, and activates the primary partition.

After the initial configuration of both the primary and alternate IBM zAware servers is complete, suppose that an administrator uses the GUI to remove device 3004 from the primary set because device 3002 alone has sufficient capacity for the data that IBM zAware needs to store. This action causes a mismatch between the primary set and alternate set of storage devices that IBM zAware detects and corrects only when the alternate partition is activated:

1. When the alternate partition is activated, the alternate IBM zAware server detects that device 9114, which contains a copy of the data from removed device 3004, is still listed as an in-use device in the alternate set of storage.
2. To correct this mismatch, the alternate IBM zAware server automatically removes device 9114 from its storage configuration and issues message AIFP0012I with device ID 9114.

Although this example assumes that the alternate server detected the removal of a device from the primary set of storage devices, the reverse is also possible; when the primary partition is activated, the primary IBM zAware server can detect and correct a mismatch that results from the removal of a device from the alternate set of storage devices.

System action: The active IBM zAware server does not use the removed device identified by *device_id*.

Response: None. If you need additional information about configuring storage for primary and alternate IBM zAware partitions, see “Example: Storage configuration for multiple IBM zAware partitions” on page 42.

AIFP0013E Persistent storage is not available because one or more devices (*total_missing*) are no longer available. IBM zAware operations cannot continue until corrective action is taken for each of the unavailable devices.

Explanation: One or more storage devices that were previously in use by IBM zAware are no longer available. The variable in the message text, *total_missing*, indicates how many devices are no longer available. In-use storage devices can become unavailable for these reasons:

- The device is no longer attached to the IBM zAware partition. It might have been removed or disconnected through storage operations that are not provided through the Data Storage page of the IBM zAware GUI, such as:

- Replacing the I/O definition file (IODF) for the host system with an IODF that does not contain the in-use storage devices for IBM zAware.
- Using the Support Element (SE) to take offline one or more channel paths (CHPIDs) for storage devices or for the network through which those devices are connected to the IBM zAware partition.

Otherwise, the storage device might be disconnected or damaged such that the host system cannot connect to it.

- The number of devices that are in use by the primary IBM zAware server no longer matches the number of devices that have been added to the alternate IBM zAware server. When your installation configures primary and alternate IBM zAware servers, the content of the primary storage devices are copied to the alternate storage devices through the replication method of your choice. For replication to be successful, the number of storage devices in the primary set must match the number of devices in the alternate set.

System action: When an in-use storage device becomes unavailable, IBM zAware operations stop. To a user of the IBM zAware GUI, the GUI appears to hang. On the SE for the IBM zAware host system, hardware messages indicate input/output (I/O) problems related to the loss of access to physical storage devices.

Response: When access to in-use storage devices is lost and the GUI appears to hang, use the System Activity display for the IBM zAware partition to check processor utilization and processor weights for the IBM zAware partition. To access the System Activity display, use the **Monitors Dashboard** task in the Hardware Management Console (HMC) for the IBM zAware host system. If the partition is not using any cycles, deactivate and reactivate the partition.

- If the partition does not successfully reactivate or still appears to be unresponsive, report the problem to IBM Support by generating a Type V Viewable PMH (PMV) record.
- If you can successfully log in to the IBM zAware GUI as an administrator, the GUI displays the Data Storage page with message AIFP0013E. Corrective measures depend on which circumstance caused the device to become unavailable. Before you take any action, however, you need to determine which device is no longer available and, if your installation is periodically backing up IBM zAware data, which equivalent device contains the replicated data.
 - If the device is no longer attached to the partition:
 - If possible, try to reattach the device and reactivate the IBM zAware partition.
 - If the device cannot be reattached, you must replace it with an equivalent device containing a backup copy of the data that was stored on the unavailable device. Use the **Add and Remove Devices** function on the Data Storage

page to replace the unavailable devices with their equivalents. Make sure that you select the “Preserve data” option when adding any replacement devices. Ordinarily, IBM zAware formats and initializes devices to be added to its persistent storage, thus overwriting the data on those devices; using the “Preserve data” option ensures that IBM zAware does not overwrite the replicated data when adding the device.

- If your installation does not have backup copies of IBM zAware data, you must deactivate the IBM zAware partition and reconfigure the IBM zAware environment.
- If IBM zAware detected a mismatch between the primary and alternate sets of storage devices:
 - If the mismatch resulted from the removal of a device, you do not need to take any corrective action.
 - If the mismatch resulted from the addition of a device, you need to determine which set— the primary or alternate— has the additional device, and add its equivalent to the other set. The size of a primary device and the size of its alternate device must match. Use the **Add and Remove Devices** function on the Data Storage page to add the equivalent device to the appropriate set, using the “Preserve data” option.

AIFP0015I IBM zAware rejected a request to add a persistent storage device, *device_id*, to the list of in-use devices. The request is rejected because the current IBM zAware storage configuration is missing one or more storage devices, as indicated by message AIFP0013E, and the requested device does not contain a backup copy of the data that was stored on one of those missing devices.

Explanation: When IBM zAware issues message AIFP0013E to indicate that one or more in-use storage devices are missing, an administrator cannot successfully add previously unused storage devices until all of the missing devices either have been reattached to the IBM zAware partition, or have been replaced with equivalent devices containing replicated data. The request to add the persistent storage device *device_id* is rejected because that device does not contain a backup copy of the data that was stored on one of the missing devices.

System action: IBM zAware does not add *device_id* to the list of in-use devices, and reissues message AIFP0013E. IBM zAware operations cannot continue until corrective action is taken for each of the missing devices.

Response: If you were attempting to replace a missing device with an equivalent device that contains

replicated data, check the device ID to verify that you are adding the correct replacement device and retry the request. Otherwise, follow the instructions for message AIFP0013E to correct the IBM zAware storage configuration.

AIFP0016E Persistent storage device *device_id* is a duplicate of storage device *device_id*. IBM zAware operations cannot continue until one of these devices is removed through the Data Storage page of the IBM zAware GUI.

Explanation: When your installation sets up replication to have a backup copy of IBM zAware data available, a storage administrator must define physically separate but equivalent sets of storage devices:

- One set for IBM zAware to use during normal operations.
- A backup set to contain replicated data.

Although both sets of devices are displayed through the IBM zAware graphical user interface (GUI) as available for use, initially an administrator can add only the set of devices that are designated for normal operations. If the backup devices are added during initial configuration of IBM zAware, replication cannot be successful because IBM zAware will use the backup devices to store its data.

After successful replication, however, an administrator can add a backup device, but only when its equivalent in-use device is no longer part of the IBM zAware storage configuration. Message AIFP0016E is issued when an administrator uses the IBM zAware GUI to add a backup device that contains the same data as a device that is currently in use. The device IDs supplied in the message text indicate the device number of the backup and its equivalent in-use storage device.

Consider the following example, for which a storage administrator has defined two sets of 3390 DASD for IBM zAware:

- Devices 3001 through 3005 are reserved to contain data that IBM zAware requires for normal operations.
 - Devices 9110 through 9115 are reserved to contain backup copies of the data from in-use devices 3001-3005.
1. Through the IBM zAware GUI, the administrator initially configures IBM zAware to use only devices 3002 and 3004.
 2. Through other tools or interfaces, the administrator also sets up replication such that the content of device 3002 is periodically copied to device 9112, and the content of device 3004 is copied to device 9114.

3. After successful replication, if an administrator adds backup device 9112 to the storage configuration while device 3002 is in use, IBM zAware detects the duplicate devices and issues message AIFP0016E.

System action: IBM zAware operations cannot continue until one of these devices is removed through the Data Storage page of the IBM zAware GUI.

Response: With a user ID assigned to the Administrator role, use the **Add and Remove Devices** function on the Data Storage page to remove one of the identified devices from the IBM zAware storage configuration.

AIFP0018W *resource* **shortage. number percent usage detected. An administrator should determine whether additional capacity can be added, or usage reduced.**

Explanation: IBM zAware detected that the current usage of either storage or memory, as indicated by the variable *resource* in the message text, has reached a level at which corrective action might be required to avoid a critical shortage. The variable *number* indicates the percentage of storage or memory that is currently in use.

A storage shortage might require an administrator to take corrective action. A memory shortage can be a temporary condition that is the result of a relatively sudden increase in activity; for example, when IBM zAware is processing a training request in addition to processing message traffic from monitored clients. In this case, the memory shortage might be resolved without any intervention.

System action: IBM zAware continues operating, periodically reissuing this message until corrective action resolves the storage or memory shortage. If the shortage reaches a critical threshold, IBM zAware begins to issue message AIFP0019E, with greater frequency.

Response: Corrective action depends on the type of resource shortage.

For a storage shortage

- Consider reducing the number of monitored systems that are currently connected.
- Check the Data Storage Devices table on the Data Storage page to determine whether any additional devices are available. Use **Add and Remove Devices** to add devices to the IBM zAware storage configuration.
- Check the retention settings on the **Analytics** tab on the Configure Settings page. Reducing the retention times for instrumentation data, training models, or analysis results might help to prevent future storage shortages, but the effect is not immediate.

For a memory shortage

- Consider reducing the number of monitored systems that are currently connected.
- Check the Training Sets page to determine whether any training requests are in progress or queued for processing; if so, the increase in memory usage might be temporary. Check the Notifications page for additional occurrences of message AIFP0018W, or for message AIFP0019E. If the percent of memory in use continues to increase, consider cancelling one or more of the queued training requests.

AIFP0019E *Critical resource* **shortage. number percent usage detected. An administrator should determine whether additional capacity can be added, or usage reduced.**

Explanation: IBM zAware detected that the current usage of either storage or memory, as indicated by the variable *resource* in the message text, has reached a critical threshold. The variable *number* indicates the percentage of storage or memory that is currently in use.

A critical storage shortage requires an administrator to take immediate corrective action. In contrast, a memory shortage might be a temporary condition that is the result of a relatively sudden increase in activity; for example, when IBM zAware is processing a training request in addition to processing message traffic from monitored clients. In this case, the memory shortage might be resolved without any intervention.

System action: IBM zAware continues operating, frequently reissuing this message until corrective action resolves the storage or memory shortage. If the shortage exceeds this critical threshold, results are unpredictable.

Response: Corrective action depends on the type of resource shortage.

For a critical storage shortage

1. Immediately reduce the number of monitored systems that are currently connected.
2. Use **Add and Remove Devices** on the Data Storage page to add available devices to the IBM zAware storage configuration.
3. Check the retention settings on the **Analytics** tab on the Configure Settings page. Reducing the retention times for instrumentation data, training models, or analysis results might help to prevent future storage shortages, but the effect is not immediate.

For a critical memory shortage

- Consider reducing the number of monitored systems that are currently connected.

- Check the Training Sets page to determine whether any training requests are in progress or queued for processing; if so, the increase in memory usage might be temporary. Check the Notifications page for additional occurrences of message AIFP0019E. If the percent of memory in use continues to increase, consider cancelling one or more of the queued training requests.
- If necessary, use the Storage Information task to view more information about the current memory usage for the IBM zAware partition. The Storage Information task is available through the CPC Operational Customization tasks list in the Support Element (SE) for the IBM zAware host system.
For information about changing the memory resources defined for a logical partition, see *zEnterprise System PR/SM Planning Guide*, SB10-7156.

AIFT0001I A request to build a model for *sysplex.system* started on *date_time*.

Explanation: IBM zAware started to process a queued request to build a model for the monitored client identified by the variable *sysplex.system*. This request can be either a training operation that IBM zAware schedules automatically at the end of the training interval, or a training operation that an administrator requested through the **Request Training** action on the Training Sets page in the IBM zAware graphical user interface (GUI). The variable *date_time* indicates when IBM zAware began to process the request.

System action: IBM zAware continues to process the training request.

Response: None required. To view the current status and progress of this training request, check the Training Progress column in the Monitored Systems table on the Training Sets page. Periodically click **Refresh** to display the most recent training status.

AIFT0002I A request to build a model for *sysplex.system* completed successfully on *date_time*.

Explanation: IBM zAware successfully processed a request to build a model for the monitored client identified by the variable *sysplex.system*. The variable *date_time* indicates when IBM zAware finished processing the request. The resulting model of system behavior replaces the prior model, if any, for this system.

System action: IBM zAware begins using the new model to identify changes in message patterns for the monitored client.

Response: None required. To view information about

the new model through the IBM zAware graphical user interface (GUI):

1. Navigate to the Training Sets page and select the system.
2. From the Actions list, select **Manage Model Dates** to open the Manage Model Dates page.
3. Select **Current Model Dates** from the Model dates list.

AIFT0003I An IBM zAware administrator cancelled a queued request to build a model for *sysplex.system*. The request was cancelled on *date_time*.

Explanation: Through the IBM zAware graphical user interface (GUI), an administrator cancelled a queued request to build a model for the monitored client identified by the variable *sysplex.system*. This request can be either a training operation that IBM zAware schedules automatically at the end of the training interval, or a training operation that an administrator requested through the **Request Training** action on the Training Sets page in the GUI.

System action: IBM zAware discards the training request on the date and time indicated by the variable *date_time*. If a model for this system exists already, IBM zAware uses that model for analysis. If a model for this system does not exist, IBM zAware cannot provide any analytical data for this system.

Response: None required. If a model does not exist for this system, consider resubmitting the training request so analysis can start shortly after the model is built. If you do not manually request training, IBM zAware automatically schedules a training request according to the analytics configuration settings.

AIFT0004E A request to build a model for *sysplex.system* failed on *date_time*. On the Notifications page, look for additional error messages that provide more detail about the cause of the failure and provide possible corrective actions.

Explanation: IBM zAware started to process a queued request to build a model but failed to complete the training operation. The training request, for the monitored client identified by *sysplex.system*, failed at *date_time*.

System action: IBM zAware continues processing other requests, if any.

Response: On the Notifications page, look for additional error messages that provide more detail about the cause of the failure. Follow the corrective actions that are provided for those additional messages.

AIFT0101I A request to build a model for *sysplex.system* did not complete successfully because the date range did not contain any days for which data is available for training. If you are building an initial model from priming data, send additional priming data within the training period date range and retry the training request. If you are replacing an existing model, the action required to resolve this error depends on various factors. See the user response for this message.

Explanation: IBM zAware attempted to create a model of system behavior for the monitored client identified by *system_name*. This training process was not successfully completed because data was not available for the dates in the training period.

System action: If a model for this monitored client already exists, IBM zAware uses it to analyze the current data from the monitored client. If a model does not exist, IBM zAware is not able to analyze current data; in this case, the bar graph for *system_name* on the **Analysis** page indicates that data is not available.

Response: Take one of the following actions with a user ID that is assigned to the Administrator role.

- If an administrator is priming IBM zAware with prior data for the system and a model does not exist yet, use the z/OS bulk load client for IBM zAware to send additional days of console logs for this system. After assigning the additional priming data, go to the **Administration > Training Sets** page and select the **Request Training** action to rebuild the system model.
- If an administrator modified the default training set such that days representing normal system activity have been excluded from the training period:
 1. Go to the **Administration > Training Sets** page, select the **Manage Model Dates** action, and select **Next Training Period Model Dates** to view and adjust the model dates.
 2. Select the date in the **Excluded Days** field and click **Remove**; repeat as necessary to re-add excluded dates to the model.
 3. Return to the **Training Sets** page and select the **Request Training** action to rebuild the system model.
- If an administrator modified the default training period but more days are required to build the model:
 1. Go to the **Administration > Configuration > Analytics** page.
 2. Increase the Training period value, and apply the change. This new value applies to all monitored clients. For new a training value to take effect for currently connected clients, you need to stop and reconnect those clients.

3. After the system is connected, go to the **Administration > Training Sets** page and select the **Request Training** action to rebuild the system model.

AIFT0102I A request to build a model for *system_name* did not complete successfully. Analysis of the data did not result in a usable pattern because of insufficient training set data. If you are building an initial model from priming data, send additional priming data and retry the training request. If you are replacing an existing model, the action required to resolve this error depends on various factors. See the user response for this message.

Explanation: IBM zAware attempted to create a model of system behavior for the monitored client identified by *system_name*. This training process was not successfully completed because the data for the model did not satisfy the requirements for successfully building a system model. For information about message traffic requirements for successfully building models of system behavior, see Chapter 8, “Planning to create IBM zAware models,” on page 57.

System action: IBM zAware removes the training request from the queue. If a model for this system exists already, IBM zAware uses that model for analysis. If a model for this system does not exist, IBM zAware cannot provide any analytical data for this system.

Response: Take one of the following actions with a user ID that is assigned to the Administrator role.

- If an administrator is priming IBM zAware with prior data for the system and a model does not exist yet, use the z/OS bulk load client for IBM zAware to send additional days of console logs for this system. After assigning the additional priming data, go to the **Administration > Training Sets** page and select the **Request Training** action to rebuild the system model.
- If a model was previously created and an administrator changed the days selected to be part of the training set, restore the original dates and request IBM zAware to rebuild the model.
 1. Go to the **Administration > Training Sets** page, select the **Manage Model Dates** action, and select **Next Training Period Model Dates** to view and adjust the model dates.
 2. Select the date in the **Excluded Days** field and click **Remove**; repeat as necessary to re-add excluded dates to the model.
 3. Return to the **Training Sets** page and select the **Request Training** action to rebuild the system model.

- If a model was previously created and an administrator changed the training period, restore the original value and request IBM zAware to rebuild the model.
1. Go to the **Administration > Configuration > Analytics** page.
 2. Increase the Training period value, and apply the change. This new value applies to all monitored clients. For new a training value to take effect for currently connected clients, you need to stop and reconnect those clients.
 3. After the system is connected, go to the **Administration > Training Sets** page and select the **Request Training** action to rebuild the system model.
- If a model was created as a result of the immediately previous training request (that is, 30 days ago, if your installation is using the default training interval), you can ignore this message as long as you are confident that the prior model still represents the current system behavior. If you have changed the workload on the system, however, consider increasing the training period or adding more training set data, and retrying the training request.
 - If the existing model was created over 60 days ago and one or more training attempts have failed, contact IBM Support.

AIFT0103I A request to build a model for *system_name* did not complete successfully because the data available for training did not contain a sufficient number of intervals with the minimum number of unique message IDs. If you are building an initial model from priming data, send additional priming data and retry the training request. If you are replacing an existing model, increase the number of days in the training set by modifying the configuration value for the training period and retry the training request.

Explanation: IBM zAware attempted to create a model of system behavior for the monitored client identified by *system_name*. This training process was not successfully completed because the data for the model did not satisfy the requirements for successfully building a system model. For information about message traffic requirements for successfully building models of system behavior, see Chapter 8, "Planning to create IBM zAware models," on page 57.

System action: IBM zAware removes the training request from the queue. If a model for this system exists already, IBM zAware uses that model for analysis. If a model for this system does not exist, IBM zAware cannot provide any analytical data for this system.

Response: Take one of the following actions with a

user ID that is assigned to the Administrator role.

- If an administrator is priming IBM zAware with prior data for the system and a model does not exist yet, use the z/OS bulk load client for IBM zAware to send additional days of console logs for this system. After assigning the additional priming data, go to the **Administration > Training Sets** page and select the **Request Training** action to rebuild the system model.
 - If a model was previously created, increase the length of the training period and request IBM zAware to rebuild the model.
1. Go to the **Administration > Configuration > Analytics** page.
 2. Increase the Training period value, and apply the change. This new value applies to all monitored clients. For new a training value to take effect for currently connected clients, you need to stop and reconnect those clients.
 3. After the system is connected, go to the **Administration > Training Sets** page and select the **Request Training** action to rebuild the system model.

If the error is not resolved through one of these actions, the message traffic for this system does not provide sufficient information for IBM zAware to construct patterns. This system cannot be an IBM zAware monitored client.

AIFT0104I Starting on *date_time*, IBM zAware successfully received *number* lines of data in which *number* lines contained messages. The received data can be either current OPERLOG data from a monitored client or priming data for one or more clients.

Explanation: IBM zAware received either current operations log (OPERLOG) data from one z/OS client, or priming data for one or more z/OS monitored clients. This message indicates when IBM zAware started receiving the data, how many lines of data were successfully received, and how many of these lines contained messages.

System action: IBM zAware receives and stores the data.

Response: None required. For priming data, if you want to verify that IBM zAware has received all of the data sent through the z/OS bulk load client, check the system log (SYSLOG) of the z/OS priming system for IXG38x or IXG37x messages that report the transfer of data between the z/OS system logger and the IBM zAware server.

AIFT0105E Starting on *date_time*, IBM zAware received *number* lines of data in which *number* lines contained messages. A significant number of lines in the received data do not contain valid message IDs. The received data can be either current OPERLOG data from a monitored client or priming data for one or more clients. Depending on the type of received data, either check the OPERLOG data, or check the z/OS bulk load client input data sets to make sure they contain priming data in the required format.

Explanation: IBM zAware received either current operations log (OPERLOG) data from one z/OS client, or priming data for one or more z/OS monitored clients. This message indicates when IBM zAware started receiving the data, how many lines of data were successfully received, and how many of these lines contained messages. A significant amount of this data did not contain valid message identifiers (IDs). For priming data, a likely cause is that the priming data does not conform to the required hardcopy log 2-digit year (HCL) or 4-digit year (HCR) format.

System action: IBM zAware receives and stores the data containing messages.

Response: Corrective action depends on the type of received data.

- For current OPERLOG data, check the OPERLOG data for systems connecting at *date_time*. Make sure that the OPERLOG configuration conforms to the requirements listed in Chapter 12, “Configuring z/OS monitored clients to send data to the IBM zAware server,” on page 91.
- For priming data, check the job used to run the z/OS bulk load client for IBM zAware on the z/OS priming system. Make sure that the input data sets are sequential and contain SYSLOG data in the appropriate format, and rerun the z/OS bulk load client to resend the priming data.

AIFT0107I IBM zAware successfully processed *number* lines of OPERLOG data in which *number* lines contained messages.

Explanation: IBM zAware issues this message when a monitored client stops sending operations log (OPERLOG) data. A client stops sending data when the connection between the client and IBM zAware ends, or when the IBM zAware analytics engine is stopped or recycled.

The message text indicates how many lines of OPERLOG data were successfully processed while the client was connected, and how many of these lines contained messages.

System action: Unless the analytics engine was

intentionally stopped through the System Status page in the IBM zAware graphical user interface (GUI), IBM zAware continues normal operations.

Response: None required. Unless the monitored client was intentionally disconnected through the SETLOGR command, you might need to take corrective action.

- If the client was unintentionally disconnected, check the system log (SYSLOG) of the z/OS system for IXG38x or IXG37x messages that report communication problems between the z/OS system logger and the IBM zAware server.
- If the client was disconnected because the IBM zAware analytics engine was stopped or recycled, you might need to issue the SETLOGR command to reconnect the system. When z/OS monitored clients are disconnected from the server, they automatically attempt to reconnect and continue to buffer data for approximately 10 minutes. If the analytics engine is restarted within that time, the z/OS system reconnects and sends the buffered data to the IBM zAware server. If the z/OS system times out before the analytics engine is restarted, any buffered data is lost and you must manually reconnect the system.

AIFT0150E IBM zAware attempted to access storage that it had been using, but the attempt failed because of an I/O read error. Possible causes of this error include an access problem with the physical storage device, a corrupted file, or other read errors. Investigate and correct the problem with the storage device and reactivate the IBM zAware partition.

Explanation: The IBM zAware server attempted to access storage that it had been using, but the attempt failed because of an I/O read error. Possible causes of this error include an access problem with the physical storage device, a corrupted file, or other read errors.

System action: The IBM zAware server cannot access its storage.

Response:

1. Ensure that the storage volumes assigned to the IBM zAware partition are physically connected to the IBM zAware host system.
2. Through the Hardware Management Console (HMC), deactivate and activate the IBM zAware partition after access to storage is corrected.

a. Deactivate the partition:

- 1) Stop the data transmission from monitored clients. Use the SETLOGR command on each z/OS system to prevent the systems from attempting to reestablish the TCP/IP connection to the IBM zAware server.

SETLOGR FORCE,ZAIQUIESCE,ALL

For information about the **SETLOGR** command and the authority required to issue that command, see *z/OS MVS System Commands*, SA22-7627.

- 2) Deactivate the IBM zAware partition. Use the **Deactivate** task in the Hardware Management Console (HMC). For authorization requirements and other information about the **Deactivate** task, see the **System z HMC and SE (Version 2.12.1) Information Center** at <http://pic.dhe.ibm.com/infocenter/hwmca/v2r12m1/index.jsp>

- b. Activate the partition.

The following steps describe one method of activating the partition through the HMC:

- 1) Select the image for the IBM zAware partition.
- 2) From the **Daily** task group, open the **Activate** task. The Activate Task Confirmation window is displayed.
- 3) Review the confirmation text to decide whether to proceed with the task. If you want to continue this task, click **Yes**. The Activate Progress window is displayed indicating the progress of the activation and the outcome.
- 4) Click **OK** to close the window when the activation completes successfully.

Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

3. Reconnect the z/OS monitored clients that were previously connected to the IBM zAware server. To reconnect each z/OS system in your IBM zAware configuration to the server, use the **SETLOGR** command on each z/OS system.

SETLOGR FORCE,ZAICONNECT,LSNAME=SYSPLEX.OPERLOG

Existing data that is already stored might be available for display through the IBM zAware graphical user interface (GUI).

Response:

1. With a user ID that is assigned to the Administrator role, go to the **Administration > Configuration > DataStorage** page in the IBM zAware GUI. To determine whether any additional volumes are available for use, sort the Data Storage Devices table by the Status column to search for available devices. If additional volumes are available, follow the procedure in “Adding and removing storage devices” on page 145 to add these devices.
2. If additional storage devices are not available, work with your storage administrator to determine whether any additional physical volumes that are attached to the IBM zAware host system can be used. If so, complete the following steps:
 - a. Through the Hardware Management Console (HMC), deactivate the IBM zAware partition:
 - 1) Stop the data transmission from monitored clients. Use the **SETLOGR** command on each z/OS system to prevent the systems from attempting to reestablish the TCP/IP connection to the IBM zAware server.

For information about the **SETLOGR** command and the authority required to issue that command, see *z/OS MVS System Commands*, SA22-7627.

- 2) Deactivate the IBM zAware partition. Use the **Deactivate** task in the Hardware Management Console (HMC). For authorization requirements and other information about the **Deactivate** task, see the **System z HMC and SE (Version 2.12.1) Information Center** at <http://pic.dhe.ibm.com/infocenter/hwmca/v2r12m1/index.jsp>

- b. To add additional volumes to the IO configuration, use the instructions in Chapter 9, “Configuring network connections and storage for the IBM zAware partition,” on page 63.
- c. Use the HMC to activate the IBM zAware partition.

The following steps describe one method of activating the partition through the HMC:

- 1) Select the image for the IBM zAware partition.
- 2) From the **Daily** task group, open the **Activate** task. The Activate Task Confirmation window is displayed.
- 3) Review the confirmation text to decide whether to proceed with the task. If you want to continue this task, click **Yes**. The

AIFT0151E IBM zAware attempted to access storage that it had been using, but the attempt failed because of an I/O write or lock error. The probable cause of this error is insufficient storage capacity. To correct this problem, an administrator must determine whether additional storage devices can be added to increase capacity.

Explanation: The IBM zAware server has used all of the available capacity of the storage devices that are currently assigned for its use.

System action: IBM zAware fails any attempt to write additional information to storage; this information includes analysis of operations log (OPERLOG) data and system models that are created through the training process.

Activate Progress window is displayed indicating the progress of the activation and the outcome.

- 4) Click **OK** to close the window when the activation completes successfully.

Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

- d. Through the IBM zAware GUI, return to the **Administration > Configuration > DataStorage** page, and add the additional devices by following the procedure in “Adding and removing storage devices” on page 145.

- e. Reconnect the z/OS monitored clients that were previously connected to the IBM zAware server. To reconnect each z/OS system in your IBM zAware configuration to the server, use the **SETLOGR** command on each z/OS system.

SETLOGR FORCE,ZAICONNECT,LSN=SYSPLEX.OPERLOG

3. Consider using the z/OS bulk load client for IBM zAware to send any missing OPERLOG data to IBM zAware for analysis and modeling. To send data that was lost while IBM zAware did not have sufficient storage capacity to analyze and save client data, use the instructions in Chapter 13, “Creating an IBM zAware model for new z/OS monitored clients,” on page 99.

AIFT0152E IBM zAware attempted to write to storage but the attempt failed. This condition might be resolved without administrator intervention. Check the Analysis page in the IBM zAware GUI; if analysis of current data has stopped or the GUI seems to hang, deactivate and reactivate the IBM zAware partition.

Explanation: IBM zAware server attempted to write to an in-use storage device but the attempt failed. Possible causes of this error include an access problem with the physical storage device, a disk failure, contention for locks, or other error conditions.

System action: Licensed Internal Code automatically gathers and sends diagnostic information to IBM if the “Call Home” feature is enabled on the IBM zAware host system.

Response: To determine whether corrective action is required, check the **Analysis** page in the IBM zAware graphical user interface (GUI). If analysis of current data from monitored clients is in progress, no corrective action is required. If analysis of current data seems to have stopped and results are not displayed for recent intervals, deactivate and reactivate the IBM zAware partition. Complete the following steps:

1. Through the Hardware Management Console (HMC), deactivate the partition:

- a. Stop the data transmission from monitored clients. Use the **SETLOGR** command on each z/OS system to prevent the systems from attempting to reestablish the TCP/IP connection to the IBM zAware server.

SETLOGR FORCE,ZAIQUIESCE,ALL

For information about the **SETLOGR** command and the authority required to issue that command, see *z/OS MVS System Commands*, SA22-7627.

- b. Deactivate the IBM zAware partition. Use the **Deactivate** task in the Hardware Management Console (HMC). For authorization requirements and other information about the **Deactivate** task, see the **System z HMC and SE (Version 2.12.1) Information Center** at <http://pic.dhe.ibm.com/infocenter/hwmca/v2r12m1/index.jsp>

2. Activate the partition.

The following steps describe one method of activating the partition through the HMC:

- a. Select the image for the IBM zAware partition.
- b. From the **Daily** task group, open the **Activate** task. The Activate Task Confirmation window is displayed.
- c. Review the confirmation text to decide whether to proceed with the task. If you want to continue this task, click **Yes**. The Activate Progress window is displayed indicating the progress of the activation and the outcome.

- d. Click **OK** to close the window when the activation completes successfully.
- Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

3. Through the IBM zAware GUI, navigate to the **Notifications** page to determine whether IBM zAware issued another AIFT0152E message after reactivation. If IBM zAware has not issued another AIFT0152E message, continue to step 4; otherwise, skip to step 5 on page 239.

4. Repeat the following steps, as necessary, to reconnect all z/OS monitored clients, one at a time.

- a. Use the **SETLOGR** command to reconnect each z/OS monitored client.

SETLOGR FORCE,ZAICONNECT,LSNAME=SYSPLEX.OPERLOG

- b. After the client has successfully reconnected, navigate to the **Notifications** page to determine whether IBM zAware issued another AIFT0152E message after the reconnection. If IBM zAware has not issued another AIFT0152E message, continue to reconnect clients; otherwise, continue to step 5 on page 239.

- c. After you have reconnected all monitored clients, continue to step 5 on page 239.

5. Determine whether the current memory and processor resources allocated to the IBM zAware partition are sufficient for the number of monitored clients, and make any necessary adjustments.
 - a. Use the Storage Information task to view information about current memory usage for the IBM zAware partition. The Storage Information task is available through the CPC Operational Customization tasks list in the Support Element (SE) for the IBM zAware host system.
 - b. Use the System Activity display for the IBM zAware partition to view information about processor resources. To access the System Activity display, use the **Monitors Dashboard** task in the HMC for the IBM zAware host system.

To check the recommendations for memory and processor resources, see “Estimating processor and memory resources” on page 27.

For information about changing the processor and memory resources defined for a logical partition, see *zEnterprise System PR/SM Planning Guide*, SB10-7156.

6. Regardless of whether you adjusted processor or memory resources in step 5, continue to check the **Notifications** page to determine whether IBM zAware issues another AIFT0152E message. If IBM zAware has not issued another AIFT0152E message after more than 24 hours of operation, no further action is necessary; otherwise, continue to step 7.
7. Request IBM support by generating a Type V Viewable PMH (PMV) record to report this message ID and reason code.

For additional information, see Chapter 24, “Reporting IBM zAware problems to IBM,” on page 199. If you do not have a maintenance contract with IBM, use the questions at the end of that topic to collect the information that you might need to report the problem to your hardware maintenance provider.

AIFT0999E IBM zAware detected an internal error while processing a request for *system_name*. The request type is *request_type*. IBM zAware collects diagnostic data and retries the request; depending on the outcome of the second attempt, corrective action might not be required. See the message description for further details.

Explanation: While processing a request for the monitored client identified by *system_name*, IBM zAware detected an internal error. The variable *request_type* indicates the type of request that IBM zAware was processing:

Train IBM zAware was building the system model

for *system_name*. This processing can be initiated by IBM zAware based on the configured training interval value, or by an administrator who used the **Request Training** action on the **Administration > Training Sets** page.

Analyze

IBM zAware was analyzing the current operations log (OPERLOG) data that *system_name* was sending.

Upload

IBM zAware was receiving either current operations log (OPERLOG) data from *system_name*, or priming data for one or more systems. For the priming case, the variable *system_name* identifies the system on which the z/OS bulk load client for IBM zAware was run to transfer the priming data.

System action: Licensed Internal Code automatically gathers and sends diagnostic information to IBM if the “Call Home” feature is enabled on the IBM zAware host system. IBM zAware terminates the request.

For a Train request

IBM zAware does not create a model when a training request fails. If a model existed prior to the failure, IBM zAware continues to use that model for analysis and attempts to retry the failed training request on the next day (UTC). For an automated build to be scheduled, the client must be connected to the IBM zAware server.

For an Analyze or Upload request

IBM zAware immediately attempts to retry the failed request.

Response: Corrective action depends on the type of request, and on the outcome of the second attempt to process the request.

For a Train request

You can either wait for IBM zAware to retry the training request on the next day, or go to the **Administration > Training Sets** page and select the **Request Training** action to attempt to rebuild the system model immediately. If the retry attempt fails, deactivate and reactivate the IBM zAware partition and retry the training request.

For an Analyze or Upload request

If the retry attempt fails, use the appropriate **SETLOGR** commands to disconnect and reconnect *system_name* from IBM zAware, and retry the request.

1. Disconnect *system_name* from the IBM zAware server by issuing the **SETLOGR** command:


```
SETLOGR FORCE,ZAIQUIESCE,ALL
```
2. Reconnect the client by issuing the **SETLOGR** command from *system_name*:

| | |
|--|---|
| <p>SETLOGR FORCE,ZAICONNECT,LSN=SYSPLEX.OPERLOG</p> <p>3. For an Upload request only, resend priming data for <i>system_name</i> through the z/OS bulk load client for IBM zAware.</p> <p>If the request fails again, deactivate and reactivate the IBM zAware partition and retry the request.</p> <p>To deactivate and reactivate the IBM zAware partition, complete the following steps:</p> <ol style="list-style-type: none"> 1. Stop the data transmission from monitored clients. Use the SETLOGR command on each z/OS system to prevent the systems from attempting to reestablish the TCP/IP connection to the IBM zAware server. SETLOGR FORCE,ZAIQUIESCE,ALL <p>For information about the SETLOGR command and the authority required to issue that command, see <i>z/OS MVS System Commands</i>, SA22-7627.</p> <ol style="list-style-type: none"> 2. Through the Hardware Management Console (HMC), deactivate the partition: <ol style="list-style-type: none"> a. Stop the data transmission from monitored clients. Use the SETLOGR command on each z/OS system to prevent the systems from attempting to reestablish the TCP/IP connection to the IBM zAware server. SETLOGR FORCE,ZAIQUIESCE,ALL <p>For information about the SETLOGR command and the authority required to issue that command, see <i>z/OS MVS System Commands</i>, SA22-7627.</p> <ol style="list-style-type: none"> b. Deactivate the IBM zAware partition. Use the Deactivate task in the Hardware Management Console (HMC). For authorization requirements and other information about the Deactivate task, see the System z HMC and SE (Version 2.12.1) Information Center at http://pic.dhe.ibm.com/infocenter/hwmca/v2r12m1/index.jsp 3. Activate the partition. The following steps describe one method of activating the partition through the HMC: <ol style="list-style-type: none"> a. Select the image for the IBM zAware partition. b. From the Daily task group, open the Activate task. The Activate Task Confirmation window is displayed. c. Review the confirmation text to decide whether to proceed with the task. If you want to continue this task, click Yes. The Activate Progress window is displayed indicating the progress of the activation and the outcome. d. Click OK to close the window when the activation completes successfully. | <p>Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.</p> <ol style="list-style-type: none"> 4. Reconnect the monitored clients. To reconnect a z/OS system, you must issue the SETLOGR command. SETLOGR FORCE,ZAICONNECT,LSN=SYSPLEX.OPERLOG <p>If the problem persists, request IBM support by generating a Type V Viewable PMH (PMV) record to report this message ID and reason code.</p> <p>For additional information, see Chapter 24, “Reporting IBM zAware problems to IBM,” on page 199. If you do not have a maintenance contract with IBM, use the questions at the end of that topic to collect the information that you might need to report the problem to your hardware maintenance provider.</p> |
|--|---|

Appendix E. Notices

This information was developed for products and services offered in the USA.

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 grant 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*

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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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.

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 measurements 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 or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)® are 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 <http://www.ibm.com/legal/copytrade.shtml>.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linux 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.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Electronic emission notices

The following statements apply to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions contained in the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, by installation or use of this equipment other than as specified in the installation manual, or by any other unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité aux normes du ministère des Communications du Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

European Community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: 0049 (0) 7032 15-2941
email: lugi@de.ibm.com

EC Declaration of Conformity (In German)

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 89/336/EWG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336) für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

update: 2004/12/07

People's Republic of China Class A Compliance Statement

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may need to perform practical actions.

声 明

此为 A 级产品,在生活环境中,
该产品可能会造成无线电干扰。
在这种情况下,可能需要用户对其
干扰采取切实可行的措施。

Japan Class A Compliance Statement

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用する
と電波妨害を引き起こすことがあります。この場合には使用者が適切な
対策を講ずるよう要求されることがあります。 VCCI-A

Korean Class A Compliance Statement

이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니
판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의
지역에서 사용하는 것을 목적으로 합니다.

Taiwan Class A Compliance Statement

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user will be required to take adequate measures.

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Glossary

A.

advanced management module (AMM). A hardware unit that provides system-management functions for all the blade servers in a BladeCenter® chassis.

alternate HMC. A System z Hardware Management Console (HMC) that is paired with the primary HMC to provide redundancy.

See also primary HMC.

AMM. See advanced management module.

appliance. A software device that provides a narrow range of functions and generally runs on a hardware platform.

application environment. The environment that includes the software and the server or network infrastructure that supports it.

ARM-instrumented application. An application in which application response measurement (ARM) calls are added to the source code so that management systems can monitor the performance of the application. ARM is an Open Group standard.

Automate suite (Automate). The second of two suites of functionality associated with the IBM zEnterprise Unified Resource Manager. The Automate suite includes goal-oriented monitoring and management of resources and energy management.

See also Manage suite.

availability policy. A description of the availability objectives for the virtual servers and element groups that support a workload resource group. Availability objectives consist of a workload impact setting and redundancy objectives for an element group.

B.

blade. A hardware unit that provides application-specific services and components. The consistent size and shape (or form factor) of each blade allows it to fit in a BladeCenter chassis.

BladeCenter chassis. A modular chassis that can contain multiple blades, allowing the individual blades to share resources such as the management, switch, power, and blower modules.

C.

central processor complex (CPC). A physical collection of hardware that consists of main storage, one or more central processors, timers, and channels. In

the zEnterprise environment, the CPC consists of a zEnterprise mainframe and any attached IBM zEnterprise BladeCenter Extension (zBX).

See also node and zCPC.

classification rule. A rule used by System z workload resource group manager firmware and software to assign a service class.

CPC. See central processor complex.

D.

DataPower® XI50z. See IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise.

discretionary goal. A service class performance goal assigned to low priority work that does not have any specific performance goal. Work is run when system resources are available.

E.

element group. A collection of functionally equivalent, redundant virtual servers that can belong to more than one workload resource group.

ensemble. A collection of one or more zEnterprise nodes (including any attached zBX) that are managed as a single logical virtualized system by the Unified Resource Manager, through the Hardware Management Console.

ensemble member. A zEnterprise node that has been added to an ensemble.

See also node.

F.

firmware. Licensed Internal Code (LIC) that is shipped with hardware. Firmware is considered an integral part of the system and is loaded and run at power on. Firmware is not open for customer configuration and is expected to run without any customer setup.

G.

GPMP. See guest platform management provider.

guest platform management provider (GPMP). An optional suite of applications that is installed in specific z/OS, Linux, and AIX® operating system images to support platform management functions. For example, the guest platform management provider collects and aggregates performance data for virtual servers and workload resource groups.

H.

Hardware Management Console (HMC). A user interface through which data center personnel configure, control, monitor, and manage System z hardware and software resources. The HMC communicates with each central processor complex (CPC) through the Support Element. On an IBM zEnterprise 196 (z196), using the Unified Resource Manager on the HMCs or Support Elements, personnel can also create and manage an ensemble.

See also [primary HMC](#) and [alternate HMC](#).

HMC. See [Hardware Management Console](#).

hypervisor. A program that allows multiple instances of operating systems or virtual servers to run simultaneously on the same hardware device. A hypervisor can run directly on the hardware, can run within an operating system, or can be imbedded in platform firmware. Examples of hypervisors include PR/SM™, z/VM, and PowerVM® Enterprise Edition.

I.

IBM blade. A customer-acquired, customer-installed select blade to be managed by IBM zEnterprise Unified Resource Manager. One example of an IBM blade is a POWER7® blade.

IBM System z Advanced Workload Analysis Reporter (IBM zAware). Firmware consisting of an integrated set of applications that monitor software running on z/OS and model normal system behavior. IBM zAware pattern recognition techniques identify unexpected messages, providing rapid diagnosis of problems caused by system changes. Operational controls and views of analytical data are available through the IBM zAware graphical user interface (GUI).

IBM System z Application Assist Processor (zAAP). A specialized processor that provides a Java execution environment, which enables Java-based web applications to be integrated with core z/OS business applications and backend database systems.

IBM System z Integrated Information Processor (zIIP). A specialized processor that provides computing capacity for selected data and transaction processing workloads and for selected network encryption workloads.

IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise (DataPower XI50z). A purpose-built appliance that simplifies, helps secure, and optimizes XML and Web services processing.

IBM zAware. See [IBM System z Advanced Workload Analysis Reporter \(IBM zAware\)](#).

IBM zAware disaster recovery environment. An IBM zAware environment that is created expressly for disaster recovery purposes.

IBM zAware environment. A configuration that consists of an IBM zAware partition and the IBM zAware monitored clients that are sending information to the IBM zAware server that is running on the partition. The IBM zAware monitored clients do not have to run in the same IBM zAware host system that contains the partition.

IBM zAware host system. The zEC12 central processor complex (CPC) that contains the logical partition (LPAR) in which the IBM System z Advanced Workload Analysis Reporter (IBM zAware) runs.

IBM zAware model. A description of normal behavior that an IBM zAware server generates for a specific monitored z/OS system. Initially, this model is based on prior data (system and application messages) from the operations log (OPERLOG) for the z/OS system. The model is updated periodically and can be modified to include or exclude specific days of system operation. The IBM zAware server uses this model to detect system problems that are indicated in current data that the server receives from the specific z/OS system.

IBM zAware monitored client. A z/OS partition that sends OPERLOG logstream data to the IBM System z Advanced Workload Analysis Reporter (IBM zAware) for analysis. To detect problems, IBM zAware compares the system and application messages in these log files to a model of normal behavior for this z/OS system, and highlights anomalous results through the IBM zAware graphical user interface (GUI).

IBM zAware partition. The logical partition (LPAR) in the zEC12 central processor complex (CPC) in which only an IBM zAware server runs. The IBM zAware graphical user interface (GUI) provides operational controls and views of analytical data for IBM zAware monitored clients.

IBM zAware server. An instance of the IBM System z Advanced Workload Analysis Reporter (IBM zAware) that is receiving data from monitored clients.

IBM zEnterprise 114 (z114). The newest generation of the entry System z family of servers built on a new processor chip, featuring a 14-way core design with enhanced memory function and capacity, security, and on demand enhancements to support existing mainframe workloads and consolidation.

IBM zEnterprise 196 (z196). The previous generation of the System z high end family of servers built on a new processor chip, featuring a 96-way core design with enhanced memory function and capacity, security, and on demand enhancements to support existing mainframe workloads and large scale consolidation.

IBM zEnterprise BladeCenter Extension (zBX). A heterogeneous hardware infrastructure that consists of a BladeCenter chassis attached to a zEC12, z196, or z114. A BladeCenter chassis can contain IBM blades or optimizers.

IBM zEnterprise BladeCenter Extension (zBX) blade. Generic name for all blade types supported in an IBM zEnterprise BladeCenter Extension (zBX). This term includes IBM blades and optimizers.

IBM zEnterprise EC12 (zEC12). The newest generation of the System z high end family of servers built on a new processor chip, featuring a 120-way core design with enhanced memory function and capacity, security, and on demand enhancements to support existing mainframe workloads and large scale consolidation.

IBM zEnterprise System (zEnterprise). A heterogeneous hardware infrastructure that can consist of a zEC12, z196, or z114 and an attached IBM zEnterprise BladeCenter Extension (zBX), managed as a single logical virtualized system by the Unified Resource Manager.

IBM zEnterprise Unified Resource Manager. Licensed Internal Code (LIC), also known as firmware, that is part of the Hardware Management Console. The Unified Resource Manager provides energy monitoring and management, goal-oriented policy management, increased security, virtual networking, and data management for the physical and logical resources of a given ensemble.

IEDN. See intraensemble data network (IEDN).

IEDN TOR switch. See intraensemble data network (IEDN) TOR switch.

INMN. See intranode management network (INMN).

intraensemble data network (IEDN). A private high-speed network for application data communications within an ensemble. Data communications for workload resource groups can flow over the IEDN within and between nodes of an ensemble. The Unified Resource Manager configures, provisions, and manages all of the physical and logical resources of the IEDN.

intraensemble data network (IEDN) TOR switch. A top-of-rack switch that provides connectivity to the intraensemble data network (IEDN), supporting application data within an ensemble.

intranode management network (INMN). A private service network that the Unified Resource Manager uses to manage the resources within a single zEnterprise node. The INMN connects the Support Element to the zEC12, z196, or z114 and to any attached IBM zEnterprise BladeCenter Extension (zBX).

M.

Manage suite (Manage). The first suite of functionality associated with the IBM zEnterprise Unified Resource Manager. The Manage suite includes

core operational controls, installation, and configuration management, and energy monitoring.

management TOR switch. A top-of-rack switch that provides a private network connection between a zEC12, z196, or z114 Support Element and an IBM zEnterprise BladeCenter Extension (zBX).

member. See ensemble member.

N.

network interface card (NIC). A printed circuit board that plugs into a server. It controls the exchange of data over a network and provides the electronic functions for the data link protocol or access method, such as token ring or Ethernet.

NIC. See network interface card.

node. A single zEC12, z196, or z114 and any optionally attached IBM zEnterprise BladeCenter Extension (zBX). A node can be a member of only one ensemble.

See also central processor complex.

O.

optimizer. A special-purpose hardware component or appliance that can perform a limited set of specific functions with optimized performance when compared to a general-purpose processor. Because of its limited set of functions, an optimizer is an integrated part of a processing environment, rather than a standalone unit.

One example of an optimizer is the IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise.

out-of-band monitoring solution. A type of monitoring solution that runs on a dedicated server rather than relying on the use of a monitoring agent installed in the operating system. For example, the IBM System z Advanced Workload Analysis Reporter (IBM zAware) provides out-of-band monitoring because it runs in a dedicated PR/SM partition and monitors clients that run in other partitions in System z servers.

OSM. An OSA-Express channel path identifier (CHPID) type that provides connectivity to the intranode management network (INMN).

OSX. An OSA-Express channel path identifier (CHPID) type that provides connectivity to the intraensemble data network (IEDN).

P.

performance index. A number that indicates whether the performance goal for a service class was achieved, exceeded, or missed.

performance policy. A description of the performance objectives and importance of a workload resource group.

platform management. The subset of systems management focused on hardware and virtualization management.

PowerVM. See [PowerVM Enterprise Edition](#).

PowerVM Enterprise Edition (PowerVM). A hypervisor that provides a set of comprehensive systems technologies and services designed to enable aggregation and management of IBM POWER® blade resources through a consolidated, logical view.

primary HMC. The System z Hardware Management Console (HMC) through which data personnel create and manage an ensemble. This HMC owns configuration and policy information that the Unified Resource Manager uses to monitor, manage, and adjust resources for all members of this ensemble.

See also [alternate HMC](#).

private system control network (PSCN). The private subsystem of the System z servers that is controlled by a fully redundant dual-Ethernet communications network. This network provides communication to all field-replaceable units (FRUs) and hierarchic control through a mirrored system of control cards and IP addresses. The PSCN provides a means for subsystems to communicate and control the dynamic parameters of system operation. The PSCN also supports error reporting, failure data collection and recovery detection, and correction of both the internal hardware and firmware of the System z servers.

PSCN. See [private system control network](#).

R.

rack. A free-standing structure or frame that can hold multiple servers and expansion units, such as BladeCenter blades.

redundancy objectives. An availability goal that identifies the minimum number and the preferred number of virtual servers in an element group that are required to support specific function for a workload resource group. Base redundancy objectives are set in the definition of the element group, but can be temporarily modified to suit a specific workload through an optional setting in an availability policy.

response time goal. A service class performance goal that defines end-to-end response time of work requests.

S.

service class. A collection of work that has the same service goals or performance objectives, resource requirements, or availability requirements.

static power save mode. A zEC12, z196, or z114 function used for periods of low utilization or potentially when a CBU system is sitting idle waiting to take over in the event of a failure. The server uses

frequency and voltage reduction to reduce energy consumption of the system. The customer initiates static power save mode by using the HMC or Support Element or Active Energy Manager.

T.

top-of-rack (TOR) switch. A network switch that is located in the first rack of an IBM zEnterprise BladeCenter Extension (zBX).

TOR switch. See [intraensemble data network \(IEDN\) TOR switch](#) and [management TOR switch](#).

transaction. A unit of processing consisting of one or more application programs, affecting one or more objects, that is initiated by a single request.

U.

Unified Resource Manager. See [IBM zEnterprise Unified Resource Manager](#).

V.

velocity goal. A service class performance goal that defines the acceptable amount of delay for work when work is ready to run. Velocity is the measure of how fast work should run when ready, without being delayed by contention for managed resources.

virtual appliance. A prepackaged software application that provides some well-defined business workflow, making it easier to deploy a solution with minimal configuration. Many tiers of operating system and applications can be packaged as a single virtual appliance. These tiers can depend on the hardware resources of different architectures.

See also [virtual server collection](#) and [virtual server image](#).

virtual server. A logical construct that appears to comprise processor, memory, and I/O resources conforming to a particular architecture. A virtual server can support an operating system, associated middleware, and applications. A hypervisor creates and manages virtual servers.

virtual server collection. A set of virtual servers that supports a workload resource group. This set is not necessarily static. The constituents of the collection at any given point are determined by the virtual servers involved in supporting the workload resource group at that time.

See also [virtual appliance](#) and [virtual server image](#).

virtual server image. A package containing metadata that describes the system requirements, virtual storage drives, and any goals and constraints for the virtual machine (for example, isolation and availability). The Open Virtual Machine Format (OVF) is a Distributed Management Task Force (DMTF) standard that describes a packaging format for virtual server images.

See also [virtual appliance](#) and [virtual server collection](#).

virtual server image capture. The ability to store metadata and disk images of an existing virtual server. The metadata describes the virtual server storage, network needs, goals, and constraints. The captured information is stored as a virtual server image that can be referenced and used to create and deploy other similar images.

virtual server image clone. The ability to create an identical copy (clone) of a virtual server image that can be used to create a new similar virtual server.

W.

workload. The amount of application processing that a computer performs at a given time. In z/OS WLM, a workload is a customer-defined collection of work to be tracked, managed, and reported as a unit. For zEnterprise, see [workload resource group](#).

workload impact setting. A list of the virtual servers that the Unified Resource Manager is to ignore when calculating the availability status of a workload resource group. A workload impact setting is an optional part of an availability policy.

workload resource group. A collection of virtual servers that perform a customer-defined collective purpose. A workload resource group generally can be viewed as a multi-tiered application. Each workload resource group is associated with a set of policies that define performance goals.

Z.

z/VM single system image (SSI) cluster. A collection of z/VM systems (called members) that can be managed, serviced, and administered as one system within which workloads can be deployed. An SSI cluster is intended to share a set of resources among all members.

z114. See [IBM zEnterprise 114 \(z114\)](#).

z196. See [IBM zEnterprise 196 \(z196\)](#).

zEC12. See [IBM zEnterprise EC12 \(zEC12\)](#).

zAAP. See [IBM System z Application Assist Processor](#).

zBX. See [IBM zEnterprise BladeCenter Extension \(zBX\)](#).

zBX blade. See [IBM zEnterprise BladeCenter Extension \(zBX\) blade](#).

zCPC. The physical collection of main storage, central processors, timers, and channels within a zEnterprise mainframe. Although this collection of hardware resources is part of the larger zEnterprise central processor complex, you can apply energy management

policies to the zCPC that are different from those that you apply to any attached IBM zEnterprise BladeCenter Extension (zBX) or blades.

See also [central processor complex](#).

zIIP. See [IBM System z Integrated Information Processor](#).

zEnterprise. See [IBM zEnterprise System \(zEnterprise\)](#).

Unified Resource Manager. See [IBM zEnterprise Unified Resource Manager](#).

Index

A

- accessibility features
 - IBM zAware GUI 56
- adding storage devices 145, 147
- alternate partition
 - storage configuration instructions 187
- alternate server
 - storage configuration 42
- analytics engine
 - configuring 79
- API
 - See* application programming interface
- application programming interface (API)
 - GET request
 - description 214
 - syntax 214
- assigning bulkload data to a sysplex 181, 182
- assigning priming data to a sysplex 179
- assigning user to roles 137
- authenticating users 134
- authorization
 - for a GET request 215
- authorizing users 137

B

- browser
 - network connections 55
 - requirements for IBM zAware GUI 55
 - security 55
 - session timeout 53, 55, 88
- browser session timeout 141
- building a model 162

C

- canceling training 164
- client model
 - creating 99
 - planning 57
- configuration
 - requirements 19
- configuring LDAP 134

D

- disaster recovery feature code 11

E

- enabling LDAP 134
- example
 - of a GET request 214
- excluding dates from a model 161
- external storage device
 - configuring 63, 79

F

- feature code 11
- Firefox
 - supported version 55

G

- GET request
 - authorization 215
 - description 214
 - example 214
 - parameter descriptions 214
 - return codes 215
 - syntax 214
 - XML response 214
 - elements for INTERVAL 220
 - elements for LPAR 216
 - for a system 215
 - for an interval 219
 - sample for INTERVAL 223
 - sample for LPAR 218

H

- HTTP GET request
 - See* GET request

I

- IBM System z Advanced Workload Analysis Reporter
 - See* IBM zAware
- IBM zAware
 - alternate partition 187
 - alternate server 42
 - feature code 11
 - IBM zAware graphical user interface
 - See* IBM zAware GUI
 - message flood automation 4
 - message processing 4
 - overview 3
 - planning
 - backup devices 36
 - client models 57
 - configuration 19
 - estimating physical storage 38
 - example storage configuration 39, 42
 - exclusive use 36
 - memory requirements 27
 - monitored clients 19
 - networking requirements 29
 - processor resources 27
 - security 51
 - selecting storage devices 38
 - storage requirements 35
 - planning checklist 13
 - prerequisites 11
 - primary partition 187

- IBM zAware (*continued*)

- primary server 42
- procedure
 - configuring analytics engine 79
 - configuring external storage device 63
 - configuring external storage devices 79
 - configuring image profile 67
 - configuring network 63
 - configuring security 79
 - configuring z/OS monitored client 91
 - creating z/OS client models 99
 - summary of IT roles and skills 13
- IBM zAware environment
 - definition 8
- IBM zAware graphical user interface
 - See* IBM zAware GUI
- IBM zAware GUI
 - accessibility features 56
 - configuring analytics engine 79
 - configuring external storage devices 79
 - configuring security 79
 - overview 9
 - planning
 - browser requirements 55
 - network connections 55
 - security 55
 - session timeout 53, 55, 88
- IBM zAware host system
 - definition 8
- IBM zAware model
 - creating 99
 - definition 9
 - for z/OS system
 - JES3 DLOG 58
 - JES3 global 163
 - planning 57
- IBM zAware partition
 - configuring external storage device 63
 - configuring image profile 67
 - configuring network 63
 - definition 8
- IBM zAware server
 - configuring analytics engine 79
 - configuring external storage devices 79
 - configuring security 79
 - configuring z/OS client 91
 - definition 8
 - priming option
 - JES3 DLOG 58
 - priming with model data
 - procedure 99
 - priming with system data
 - planning 57
- image profile
 - configuring 67

- Internet Explorer
 - supported version 55
- IPL
 - z/OS client 97
- IT role
 - summary 13
- IT skill
 - summary 13

J

- JES3 DLOG 58
- JES3 global function 163

L

- LTPA timeout 141

M

- managing ignored messages 164
- memory requirements
 - estimating 27
- merging data 183
- message
 - ignore status 126
- message flood automation 4
- message processing 4
- messages
 - ignore during training 164
- Microsoft Internet Explorer
 - supported version 55
- model 179
- models overview 159
- monitored client
 - configuring z/OS 91
 - creating model 57
 - creating z/OS model 99
 - supported types 19
- moving systems to another sysplex 183
- Mozilla Firefox
 - supported version 55

N

- network
 - configuring 63
- networking requirements
 - planning 29

O

- operations log
 - See* OPERLOG
- OPERLOG
 - requirement 11

P

- parameter
 - for a GET request 214
- partition
 - configuring external storage device 63

- partition (*continued*)
 - configuring image profile 67
 - configuring network 63
- physical storage
 - planning 35
- planning
 - client models 57
 - configuration 19
 - monitored clients 19
- planning checklist 13
- prerequisites
 - OPERLOG 11
 - z/OS system
 - required version 11
- primary server
 - storage configuration 42
- priming data 179, 181, 182
- procedure
 - adding storage devices 145
 - configuring analytics engine 79
 - configuring external storage device 63
 - configuring external storage devices 79
 - configuring image profile 67
 - configuring network 63
 - configuring security 79
 - configuring z/OS monitored client 91
 - creating z/OS client models 99
 - removing storage devices 145
- processor resources
 - estimating 27
- project plan 13

R

- removing dates from a model 161
- removing storage devices 145, 147
- replacing the SSL certificate 130
- replication
 - backup devices 36
 - example configuration 39, 42
 - methods 39
 - of IBM zAware data 36
- requesting training 162
- recommendations 163
- restart
 - z/OS client 97
- return code
 - for a GET request 215

S

- security
 - configuring 79
 - planning 51
- session timeout 141
- sorting tables 124
- starting data collection 153
- starting the analytics engine 153
- status
 - ignore 126
- stopping data collection 153
- stopping the analytics engine 153

- storage
 - estimating 38
 - planning
 - backup devices 36
 - example configuration 39, 42
 - exclusive use 36
 - selecting devices 38
- storage device
 - adding 145
 - configuring 63
 - removing 145
- storage requirements
 - planning 35
- syntax
 - for a GET request 214
- sysplex topology 183

T

- time line
 - graphical format 122
 - text-only format 125
- training interval 159
- training overview 159
- training period 159

V

- verifying that data is available 161
- viewing a list of monitored systems 150
- viewing model dates 161
- viewing the status of monitored systems 150

X

- XML document
 - elements of INTERVAL request 220
 - elements of LPAR request 216
 - for INTERVAL request 219
 - for LPAR request 215
 - sample for INTERVAL request 223
 - sample for LPAR request 218

Z

- z/OS monitored client
 - configuring 91
 - effect of IPL or restart 97
- z/OS system
 - creating model 99
 - JES3 DLOG 58
 - JES3 global 163
 - planning to create model 57
 - planning to monitor 19
 - required version 11



Printed in USA

SC27-2623-01

