This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
CA Technologies Product References

This document references the following CA Technologies products and features:

- CA Application Performance Management (CA APM)
- CA Application Performance Management ChangeDetector (CA APM ChangeDetector)
- CA Application Performance Management ErrorDetector (CA APM ErrorDetector)
- CA Application Performance Management for CA Database Performance (CA APM for CA Database Performance)
- CA Application Performance Management for CA SiteMinder® (CA APM for CA SiteMinder®)
- CA Application Performance Management for CA SiteMinder® Application Server Agents (CA APM for CA SiteMinder® ASA)
- CA Application Performance Management for IBM CICS Transaction Gateway (CA APM for IBM CICS Transaction Gateway)
- CA Application Performance Management for IBM WebSphere Application Server for z/OS (CA APM for IBM WebSphere Application Server for z/OS)
- CA Application Performance Management for IBM WebSphere for Distributed Environments (CA APM for IBM WebSphere for Distributed Environments)
- CA Application Performance Management for IBM WebSphere MQ (CA APM for IBM WebSphere MQ)
- CA Application Performance Management for IBM WebSphere Portal (CA APM for IBM WebSphere Portal)
- CA Application Performance Management for IBM WebSphere Process Server (CA APM for IBM WebSphere Process Server)
- CA Application Performance Management for IBM z/OS® (CA APM for IBM z/OS®)
- CA Application Performance Management for Microsoft SharePoint (CA APM for Microsoft SharePoint)
- CA Application Performance Management for Oracle Databases (CA APM for Oracle Databases)
- CA Application Performance Management for Oracle Service Bus (CA APM for Oracle Service Bus)
- CA Application Performance Management for Oracle WebLogic Portal (CA APM for Oracle WebLogic Portal)
- CA Application Performance Management for Oracle WebLogic Server (CA APM for Oracle WebLogic Server)
- CA Application Performance Management for SOA (CA APM for SOA)
- CA Application Performance Management for TIBCO BusinessWorks (CA APM for TIBCO BusinessWorks)
- CA Application Performance Management for TIBCO Enterprise Message Service (CA APM for TIBCO Enterprise Message Service)
- CA Application Performance Management for Web Servers (CA APM for Web Servers)
- CA Application Performance Management for webMethods Broker (CA APM for webMethods Broker)
- CA Application Performance Management for webMethods Integration Server (CA APM for webMethods Integration Server)
- CA Application Performance Management Integration for CA CMDB (CA APM Integration for CA CMDB)
- CA Application Performance Management Integration for CA NSM (CA APM Integration for CA NSM)
- CA Application Performance Management LeakHunter (CA APM LeakHunter)
- CA Application Performance Management Transaction Generator (CA APM TG)
- CA Cross-Enterprise Application Performance Management
- CA Customer Experience Manager (CA CEM)
- CA Embedded Entitlements Manager (CA EEM)
- CA eHealth® Performance Manager (CA eHealth)
- CA Insight™ Database Performance Monitor for DB2 for z/OS®
- CA Introscope®
- CA SiteMinder®
- CA Spectrum®
- CA NetQoS® Performance Center
- CA Performance Center
Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.
Contents

Chapter 1: How to Install and Configure CA APM Cross-Enterprise  11
About CA Application Performance Management Cross-Enterprise ......................................................... 11
Summary of Installation and Configuration Procedure .................................................................................. 12
Prepare for Installation ................................................................................................................................. 12
  CA Common Services Requirements ......................................................................................................... 12
  Installation Software Prerequisites ........................................................................................................... 15
  Security Prerequisites ............................................................................................................................... 15
  Additional Prerequisites .......................................................................................................................... 17
Install and Enable the Enterprise Manager Components .............................................................................. 18
  Enterprise Manager Component Files ....................................................................................................... 19
Uninstall CE APM Components from Enterprise Manager ........................................................................... 20
Install and Enable CA APM Java Agent Components.................................................................................... 20
  Java Agent Component Files ..................................................................................................................... 23
Install the MQ Tracer (Optional) .................................................................................................................. 27
Install and Configure the CA APM Cross-Enterprise Agent ....................................................................... 28
  Install the CA APM Cross-Enterprise Agent ............................................................................................ 28
  Deploy the CA APM Cross-Enterprise Agent ............................................................................................ 31
  Configure the CA APM Cross-Enterprise Agent ....................................................................................... 34
  Start the CA APM Cross-Enterprise Agent ............................................................................................... 44
  Stop the CA APM Cross-Enterprise Agent ............................................................................................... 44
  Maintain the CA APM Cross-Enterprise Agent ......................................................................................... 44
  Deploy an Updated Version of the CA APM Cross-Enterprise Agent ....................................................... 45
Configure CA SYSVIEW .............................................................................................................................. 46
Verify the Installation .................................................................................................................................... 47

Chapter 2: Integrate CA NetMaster NM for TCP/IP with CA Introscope®  49
How You Integrate CA NetMaster NM for TCP/IP with CA Introscope® ...................................................... 49
  Verify File Locations .................................................................................................................................. 50
  Configure EPAgent ...................................................................................................................................... 50
  Confirm the Connectivity ............................................................................................................................ 51
  Configure CA NetMaster NM for TCP/IP .................................................................................................... 52
  Verify the Integration ................................................................................................................................. 53
Performance Monitoring Metrics .................................................................................................................. 53
Specify the Performance Monitoring Metrics to Send .................................................................................. 54
Chapter 3: How to use the Console to Identify Problems .......................... 57
About CA APM Cross-Enterprise Dashboards .................................................. 57
  View Dashboards in the Introscope Console .................................................. 59
  Alert Indicators ................................................................................. 59
CA APM Cross-Enterprise - Mainframe Health Overview Dashboard .................. 60
z/OS System Health Dashboard ................................................................. 62
CICS Regions Health Dashboard ................................................................. 64
CICS Transaction Groups Details Dashboard ............................................... 65
IMS Subsystems Health Dashboard ............................................................... 67
IMS Transaction Groups Health Dashboard .................................................... 69
CA Datacom Address Spaces Health Dashboard ........................................ 70
Queue Managers Health Dashboard ............................................................. 71
Websphere MQ Queues Health Dashboard .................................................... 73
TCPIP Stacks Health Dashboard ................................................................. 74
DB2 z/OS Performance Overview Dashboard ............................................... 75
DB2 z/OS Subsystem Information Dashboard ............................................... 77
DB2 z/OS CPU Activity Dashboard ............................................................ 78
DB2 z/OS Buffer Pool Activity Dashboard .................................................... 81
DB2 z/OS EDM Pool Activity Dashboard ....................................................... 84
DB2 z/OS Lock Activity Dashboard ............................................................. 86
DB2 z/OS Log Activity Dashboard ............................................................... 88
DB2 z/OS Workload Dashboard ................................................................. 90
DB2 z/OS More Information Dashboard ....................................................... 93

Chapter 4: How to Trace and Analyze Events ............................................ 97
About CA Introscope ............................................................................. 97
About Cross-Process Transaction Traces ....................................................... 98
Generating Cross-Process Transaction Traces ............................................. 100
  Enable Cross Process Transaction Tracing ............................................... 101
  Select Event Duration and Type Filters .................................................... 102
  Select CICS or IMS Filters .................................................................. 104
  Select Trace Duration, Agent Filters, and Start Trace ......................... 108
Narrow Trace by Excluding Front-End Elements ....................................... 109
Analyze Trace Results ............................................................................. 110
  Change Duration Time Intervals ............................................................ 111
  Cross-Process Traces Time Alignment .................................................. 111
About Transaction Trace View .................................................................. 112
CICS with MQ Trigger Message Example Using the Tree View .................. 117
Web Services Example Using Large Duration Time .................................. 118
CTG Example for High Suspend Time ....................................................... 118
Problematic Transaction for Unit of Work ............................................... 120
Chapter 5: CA APM Cross-Enterprise Metrics 143

About CTG CA SYSVIEW Tracer Metrics ..............................................................143
About CA Cross-Enterprise APM z/OS Metrics ..............................................144
CA SYSVIEW Metric Categories .......................................................................145
  z/OS Metrics ..................................................................................................149
  z/OS Alerts .....................................................................................................153
  z/OS Degradation Delay Analysis ..................................................................155
  z/OS Workload Manager Service Goals ..........................................................158
CICS Regions .....................................................................................................160
CICS Transaction Groups ..................................................................................163
CICS Alerts .......................................................................................................164
CICS Degradation Analysis ..............................................................................166
Datacom Address Spaces ..................................................................................167
IMS Subsystems ...............................................................................................170
IMS Transaction Groups ..................................................................................172
MQ Queue Managers .......................................................................................173
MQ Alerts ..........................................................................................................177
MQ Queues .......................................................................................................178
TCP/IP Stacks ...................................................................................................181
DB2 z/OS Subsystems Metrics .........................................................................184
  Buffer Pool ....................................................................................................184
  Distributed Activity .........................................................................................185
  EDM Pool .......................................................................................................186
  Exceptions ......................................................................................................187
General .................................................................................................................................188
Group Buffer Pool .............................................................................................................189
Locks .................................................................................................................................... 190
Log Activity .......................................................................................................................... 191
Misc ...................................................................................................................................... 191
Subsystem CPU .................................................................................................................... 193
Workload .............................................................................................................................. 194
CA NetMaster NM for TCP/IP Metric Categories ................................................................. 196
   DB2 DDF ........................................................................................................................... 197
   EE ......................................................................................................................................... 198
   IP Internals .......................................................................................................................... 199
   IP Resources ...................................................................................................................... 200
   IPSec .................................................................................................................................... 200
   Identification ....................................................................................................................... 201
   Interfaces ............................................................................................................................. 202
   Network Activity .................................................................................................................. 203
   Sockets .................................................................................................................................. 204
   Top Lists ............................................................................................................................... 205

Chapter 6: CA NetMaster NM for TCP/IP Reports ................................................................. 207
   Report Templates ................................................................................................................ 207

Appendix A: Troubleshoot CA APM Cross-Enterprise ......................................................... 209
   Problems with the SMF Socket Connection ....................................................................... 209
   Some Transactions Do Not Appear in the Transaction Trace Viewer ................................ 210
   SMF Transactions Traces Missing ...................................................................................... 211
   Correlation ID NotFound ...................................................................................................... 212
   No Data in a CA NetMaster NM for TCP/IP Metric Category ........................................... 213

Appendix B: MVS Messages .................................................................................................. 215
Chapter 1: How to Install and Configure CA APM Cross-Enterprise

This section contains the following topics:

- About CA Application Performance Management Cross-Enterprise (see page 11)
- Summary of Installation and Configuration Procedure (see page 12)
- Prepare for Installation (see page 12)
- Install and Enable the Enterprise Manager Components (see page 18)
- Install and Enable CA APM Java Agent Components (see page 20)
- Install the MQ Tracer (Optional) (see page 27)
- Install and Configure the CA APM Cross-Enterprise Agent (see page 28)
- Configure CA SYSVIEW (see page 46)
- Verify the Installation (see page 47)

About CA Application Performance Management Cross-Enterprise

CA Application Performance Management Cross-Enterprise (CA APM Cross-Enterprise) is an extension that enables cross-enterprise application performance management. This extension lets you manage application performance of distributed applications. This includes accessing mainframe backend and trace transactions from distributed applications to mainframe CICS or IMS. You can also use the extension to monitor health metrics of critical mainframe components. These mainframe components can include z/OS, TCP/IP, IBM WebSphere MQ, CA Datacom, and IBM DB2 database subsystems.

This extension increases end-to-end visibility for isolating transaction performance problems and lets you leverage existing CA SYSVIEW and CA NetMaster NM for TCP/IP performance data.

CA APM Cross-Enterprise also addresses the problems that are associated with applications that span mainframe and distributed environments. These silos have different tools, processes, and estranged teams. Use CA APM Cross-Enterprise to bridge these silos.

Familiarize yourself with the available documentation from CA APM Cross-Enterprise, CA SYSVIEW, CA Insight DPM for DB2 for z/OS, and CA APM for IBM WebSphere MQ. You can access this documentation from CA Technical Support site.

Note: When this guide refers to Enterprise Manager, it always refers to CA APM Enterprise Manager.
Summary of Installation and Configuration Procedure

The CA APM Cross-Enterprise installation and configuration have multiple steps.

Note: If you want to integrate only with CA NetMaster NM for TCP/IP, you do not have to perform these tasks.

Follow these steps:
1. Prepare for Installation Procedure (see page 12)
2. Install and Enable the Enterprise Manager Components (see page 18)
3. Install and Enable CA APM Java Agent Components (see page 20)
4. Install the MQ Tracer (Optional) (see page 27)
5. Install the CA APM Cross-Enterprise Agent (see page 28)
6. Deploy the CA APM Cross-Enterprise Agent (see page 31)
7. Configure the CA APM Cross-Enterprise Agent (see page 34)
8. Configure CA SYSVIEW (see page 46)
9. Verify the installation (see page 47)

Prepare for Installation

Before you install CA APM Cross-Enterprise, familiarize yourself with the various CA APM Cross-Enterprise installers. For more information about the Enterprise Manager and Workstation installers, see the CA APM Installation and Upgrade Guide. For more information about the Java agent installer, see the CA APM Java Agent Implementation Guide.

Additionally, verify that you have met all the necessary prerequisites.

CA Common Services Requirements

CA APM Cross-Enterprise requires the CA Common Communications Interface (CAICCI) portion of CA Commons Services. CAICCI is used to communicate between the WILYZOS address space and the CA SYSVIEW user address space, SYSVUSER, on the same z/OS host. The CA Event Notification Facility (CAIENF) address space is responsible for starting and initializing CAICCI.
CA APM Cross-Enterprise requires the following components:

- The CAIENF address space must be running.
- The SYSID() statement must be present in the CAIENF/CAICCI parameters.
- CAS9DCM3 must be installed.

CA APM Cross-Enterprise does not require that the CCITCP or CCITCPGW address spaces be active, nor does it require that PROTOCOL, NODE, and CONNECT statements be specified. However, other optional functions in base CA SYSVIEW (or other CA Technologies products) require these address spaces and definitions. (For example, the CCITCPGW address space must be active for the Cross-system Resource Monitoring feature of base CA SYSVIEW to operate.)

Note: For more information, see the CA Common Services for z/OS Installation Guide.

Set Up CAICCI for CA APM Cross-Enterprise

Use this procedure if you do not have CAICCI set up.

Note: For more information, see the CA Common Services for z/OS Installation Guide.

Follow these steps:

1. Define the CAICCI SYSID in the CAIENF parameter file or as a separate CCIPARM PDS member concatenated to ENFPARMS, using the following format:

   SYSID(sysid)

   sysid

   Specifies the CAICCI identifier.

   Limit: Eight characters

2. Depending on the release of CA Common Services, perform one of the following steps:

   - (r12 or later) Define the CAICCI data collection module (DCM), CAS9DCM3, in your CAIENF parameter file.
   - (r11 SP8) Install CAS9DCM3 into the CAIENF database using the CAS9DB utility.
Start XSXS Subtask

The XSXS (XSystem eXternal Server) subtask in the CA SYSVIEW user address space (SYSVUSER) provides the following functions:

- Interfaces with CAICCI.
- Performs the SYSVUSER portion of the communication between the SYSVUSER address space and the WILYZOS address space.

Verify that the XSXS subtask in the SYSVUSER address space is started. The CA SYSVIEW ASADMIN command display lists the subtasks and the status for each of the tasks in each of the address spaces in CA SYSVIEW. If the XSXS task is not listed as ACTIVE, start the XSXS subtask by issuing an S (START) line command next to the XSXS task.

Also, make a permanent change to ensure that the XSYS task starts up automatically when CA SYSVIEW starts. To accomplish this change, add a START XSXS command to the SYSVUSER parmlib member.

Note: For more information, see the CA SYSVIEW Performance Management Installation Guide.

Set Up Xmanager, Xnet, and Required IQL Queries

To retrieve metric data from one or more DB2 subsystems running on a single LPAR, install and configure CA Insight DPM on the same LPAR running the CA APM Cross-Enterprise Agent. As part of the installation and configuration of this software, also install and configure the Xmanager and Xnet components.

CA Insight DPM for DB2 for z/OS includes many Insight Query Language (IQL) queries. These queries can be used to gather information about CA Insight DPM or the DB2 subsystems that CA Insight DPM currently monitors. The CA APM Cross-Enterprise Agent uses several of these IQL queries through the Xmanager/Xnet interface to gather metric data. Specifically, the following IQL queries must be available and started in each CA Insight DPM instance for CA APM Cross-Enterprise Agent to monitor:

- DSQPARMS
- DSQAPMSS

Note: If multiple CA Insight agents are configured to monitor the same DB2 subsystem, each CA Insight agent must have these IQL queries available and started. Then, Cross-Enterprise APM Agent is able to retrieve metrics from this DB2 subsystem.

The DSQAPMSS IQL query is included with CA Insight DPM.

See the Compatibility Matrix on CA Support, which describes all the required releases and PTFs.
Installation Software Prerequisites

Before you install the CA APM Cross-Enterprise, verify that you have met the requirements for each component. For a complete list of the software/system requirements, see the Application Performance Management Compatibility Guide on the CA APM bookshelf. The product compatibility matrix provides a list of all supported operating environments.

The CA APM Cross-Enterprise Agent must report to a minimum of CA Enterprise Manager 9.x. The Enterprise Manager can reside on any supported operating system.

The CA APM Cross-Enterprise Agent must run on the same computer (and LPAR) as both CA SYSVIEW and CA Insight DPM.

Security Prerequisites

Before you install the CA APM Cross-Enterprise, verify that the person responsible for installing the software has the authority and meets these security requirements:

- Obtain the authorization to run a batch JCL streams.
- Establish READ, WRITE, and ALLOCATE access to the data set prefix or high-level qualifier that is used for the installation.
- Obtain a user ID with an OMVS segment and UID defined for access to UNIX System Services (USS).
- If it is determined that superuser or a UID(0) rights are not assigned:
  - Obtain the permission to mount a USS file system.
  - Establish READ access to the SAF resource SUPERUSER.FILESYS.MOUNT in the UNIXPRIV class.
- Obtain the permission to update and create directories and files in the mount point for the installation.
- If the user ID that is assigned to WILYZOS cannot be in the same group ID (GID) as the person installing the software, then CONTROL access to the SAF resource SUPERUSER.FILESYS in the UNIXPRIV class is required.
Before you can run the CA APM Cross-Enterprise, verify that the user ID that is assigned to the WILYZOS procedure (the WILYZOS user ID) has the authority and meets these security requirements:

- Has the authorization to run batch JCL streams.
- Has READ access to the data set prefix or high-level qualifier that is used for the installation.
- Has an OMVS segment and UID assigned.
- Has READ access to the installation data set high-level qualifier.
- Has permission to update and create directories and files in the mount point for the installation.
- Has READ access to the SAF resource BPX.CONSOLE in the FACILITY class. Otherwise, the WTO messages that are issued by the agent are prefixed with message ID BPXM023I.
- Recognize that support for the PassTicket authentication is required to retrieve metric data from local IBM DB2 subsystems. The WILYZOS user ID must have the permission to generate PassTickets. Refer to the documentation provided by your security vendor or refer to the IBM z/OS Security Server RACF Security Guide for information about configuring your security manager to perform PassTicket operations. Configure the Xnet component of CA Database Management Solutions for DB2 for z/OS to accept PassTicket authentication information. If PassTicket support is not configured, specify a valid user ID and password in the agent configuration file (which can potentially be a security risk).
Additional Prerequisites

Gather the following information:

- Know the computer on which your existing Enterprise Manager is installed.
- Identify these directory locations in your CA Introscope® Agent environment:
  - Application server home directory — Home directory of your application server.
  - Agent home directory — Installation directory of the CA Introscope® Agent for the application server being monitored.
  - Introscope directory — Installation directory for CA Introscope® on your Enterprise Manager computer.
  - The directory where `IntroscopeAgent.profile` is located, on each agent where you plan to implement CA APM Cross-Enterprise.
    
    The agent profile is typically in the top-level directory of the agent installation. The CE APM profile is `Introscope_Cross-Enterprise_APM.profile` and is found within `<host-location>/Cross-Enterprise_APM/config/Introscope_Cross-Enterprise_APM.profile`. The CA Introscope® Agent profile is `IntroscopeAgent.profile` and is found within `<Agent_Home>\wily\core\config\IntroscopeAgent.profile`.

- Know the components that you plan to install on each computer.

  **Note:** For more information, see [Install and Enable the Enterprise Manager Components](#) (see page 18) and [Install and Enable Java Agent Components](#) (see page 20).

- Know the proxy host name and proxy server port (if you have to provide this information to access the CA APM software download area on CA Support). If your proxy server requires authentication, you must have a valid user name and password for the proxy server.

- Verify if a firewall exists between the CA APM Cross-Enterprise extension and Enterprise Manager, open the CA APM Cross-Enterprise Extension port on the firewall. The extension connects to this port.

  **Note:** For more information, see [Configure Network Topology and Firewall Settings](#) (see page 37).
Install and Enable the Enterprise Manager Components

While you install Enterprise Manager, the installation panel, Select Monitoring Options displays a full set of monitoring options that you can select and enable. To enable and install the required components, select the CA Cross-Enterprise Application Performance Management option.

For the installation instruction for CE APM Enterprise Manager, see the CA APM Introscope Manager documentation.

Perform the following steps to enable the CA APM Cross-Enterprise monitoring option subsequent to the initial installation of Enterprise Manager.

Follow these steps:

1. Copy the contents from the `<EM_Home>\examples\Cross-Enterprise_APM` directory to the respective directories within the `<EM_Home>` directory.

2. Verify that the files are in the following directories:

   - `<EM_Home>\config\modules\Cross-Enterprise_APM_SYSVIEW_Management_Module.jar`
   - `<EM_Home>\config\modules\Cross-Enterprise_APM_DB2zOS_Management_Module.jar`
   - `<EM_Home>\config\modules\NetMasterAgent_Management_Module.jar`
   - `<EM_Home>\ext\ddtv\Cross-Enterprise_APM_SYSVIEW.typeviewers.xml`
   - `<EM_Home>\ext\ddtv\Cross-Enterprise_APM_SYSVIEWMQObjects-typeviews.xml`
   - `<EM_Home>\ext\ddtv\NetMasterAgent_typeviewers.xml`
   - `<EM_Home>\product\enterprisemanager\features\com.wily.introscope.ext.sysview.em.extensions.feature <version>.jar`
   - `<EM_Home>\product\enterprisemanager\plugins\com.wily.introscope.ext.sysview.common.<version>.jar`
   - `<EM_Home>\product\enterprisemanager\plugins\com.wily.introscope.ext.sysview.common.<version>.jar`
   - `<EM_Home>\scripts\Cross-Enterprise_APM_SYSVIEW.js`
   - `<EM_Home>\scripts\Cross-Enterprise_APM_Insight.js`
   - `<EM_Home>\scripts\Cross-Enterprise_APM_SYSVIEWMQQueueManagerAggregation.js`
   - `<EM_Home>\scripts\Cross-Enterprise_APM_SYSVIEWMQQueueManagerTypeviewers.js`
   - `<EM_Home>\ws-plugins\com.wily.introscope.ext.sysview.common.<version>.jar`
   - `<EM_Home>\ws-plugins\com.wily.introscope.ext.sysview.common.<version>.jar`
   - `<EM_Home>\ws-plugins\com.wily.introscope.ext.sysview.workstation.<version>.jar`
   - `<EM_Home>\ws-plugins\features\com.wily.introscope.ext.sysview.workstation.extensions.feature <version>.jar`
   - `<EM_Home>\ws-plugins\features\com.wily.introscope.ext.sysview.workstation.extensions.feature <version>.jar`

3. Restart the Introscope Enterprise Manager.
## Enterprise Manager Component Files

The following table lists all the Enterprise Manager component files for the CA APM Cross-Enterprise.

<table>
<thead>
<tr>
<th>File</th>
<th>Directory structure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-Enterprise_APM_SYSVIEW_Management_Module.jar</td>
<td>\config\modules</td>
<td>Management modules and dashboards</td>
</tr>
<tr>
<td>Cross-Enterprise_APM_DB2zOS_Management_Module.jar</td>
<td>\config\modules</td>
<td>Management modules and dashboards</td>
</tr>
<tr>
<td>Cross-Enterprise_APM_SYSVIEW.typeviewers.xml</td>
<td>\ext\ddtv</td>
<td>Tab views that appear in the CA Introscope® Workstation</td>
</tr>
<tr>
<td>Cross-Enterprise_APM_SYSVIEW.MQObjects-typeviewers.xml</td>
<td>\ext\ddtv</td>
<td>Tab views that appear in the CA Introscope® Workstation</td>
</tr>
<tr>
<td>Cross-Enterprise_APM_SYSVIEW.js</td>
<td>\scripts</td>
<td>JavaScripts for calculated metrics</td>
</tr>
<tr>
<td>Cross-Enterprise_APM_Insight.js</td>
<td>\scripts</td>
<td>JavaScripts for calculated metrics</td>
</tr>
<tr>
<td>Cross-Enterprise_APM_SYSVIEW.MQQueueManagerAggregation.js</td>
<td>\scripts</td>
<td>JavaScripts for calculated metrics</td>
</tr>
<tr>
<td>Cross-Enterprise_APM_SYSVIEW.MQQueuesAggregation.js</td>
<td>\scripts</td>
<td>JavaScripts for calculated metrics</td>
</tr>
<tr>
<td>feature.xml</td>
<td>\product-enterprisemanager\features\com.wily.introscope.ext.sysview.em.extensions.feature_&lt;version&gt;</td>
<td>CA EEM plug-ins for the tracer filter</td>
</tr>
<tr>
<td>com.wily.introscope.ext.sysview.common_&lt;version&gt;.jar</td>
<td>\product\enterprisemanager\plugins</td>
<td>Enterprise Manager plug-ins for the tracer filter</td>
</tr>
<tr>
<td>com.wily.introscope.ext.sysview.em_&lt;version&gt;.jar</td>
<td>\product\enterprisemanager\plugins</td>
<td>Enterprise Manager plug-ins for the tracer filter</td>
</tr>
<tr>
<td>feature.xml</td>
<td>\ws-plugins\features\com.wily.introscope.ext.sysview.workstation.extensions.feature_&lt;version&gt;</td>
<td>Workstation plug-ins for tracer filter</td>
</tr>
<tr>
<td>com.wily.introscope.ext.sysview.common.nl1_&lt;version&gt;.jar</td>
<td>\ws-plugins</td>
<td>Workstation plug-ins for tracer filter</td>
</tr>
<tr>
<td>com.wily.introscope.ext.sysview.common_&lt;version&gt;.jar</td>
<td>\ws-plugins</td>
<td>Workstation plug-ins for tracer filter</td>
</tr>
</tbody>
</table>
Install and Enable CA APM Java Agent Components

<table>
<thead>
<tr>
<th>File</th>
<th>Directory structure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.wily.introscope.ext.sysview.workstation_&lt;version&gt;.jar</td>
<td>\ws-plugins</td>
<td>Workstation plug-ins for tracer filter</td>
</tr>
</tbody>
</table>

Uninstall CE APM Components from Enterprise Manager

To uninstall CE APM components from Enterprise Manager, the following steps are necessary.

**Note:** For additional information refer to the *CA APM Installation and Upgrade Guide*.

**Follow these steps:**
1. Stop the Enterprise Manager if it is running.
2. Remove all the CA APM Cross-Enterprise-related files from the `<EM_Home>` directory which are listed under Enterprise Manager Component Files.

Install and Enable CA APM Java Agent Components

The following steps are necessary to install the CA APM Java Agent files.

**Follow these steps:**
1. If the CTG, http, and Webservices tracers are not selected at installation time, copy the jar files from `<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext` to `<Agent_Home>\wily\core\ext`.
2. Select and run the Java agent installer for your environment.

**Note:** For more information, see the *CA Application Performance Management Java Agent Implementation Guide*.

After you run the installer, verify that these files are in the following directories:

- `<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext\com.wily.introscope.ext.sysview.agent_<version>.jar`
- `<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext\ctg-tracer.jar`
- `<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext\WS-SYSVIEW-Tracer.jar`
- `<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext\http-tracer.jar`
3. Enable the CTG CA SYSVIEW tracer:
   a. Copy the ext\com.wily.introscope.ext.sysview.agent_<version>.jar and ext\ctg-tracer.jar files from the <Agent_Home>\wily\examples\Cross-Enterprise_APM\ext directory to the existing <Agent_Home>\wily\core\ext directory of the Introscope agent.
   b. Verify that the ctg-tracer.jar and com.wily.introscope.ext.sysview.agent_<version>.jar files are located in the <Agent_Home>\wily\core\ext directory.
   c. Verify that the CTG_ECI_Tracer_For_Sysview.pbd file is in the <Agent_Home>\wily\core\config directory. Make the following edits to the IntroscopeAgent.profile file in the <Agent_Home>\wily\core\config directory:
      - Append CTG_ECI_Tracer_For_Sysview.pbd to the introscope.autoprobe.directives property.
        For example:
        introscope.autoprobe.directivesFile=CTG_ECI_Tracer_For_Sysview.pbd,hot deploy.
      - Edit <EM hostname> to point to the Enterprise Manager computer.
        For example:
        introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=<EM hostname>.
   d. Add the ctgclient.jar file to the classpath. For example, "C:\Program Files\IBM\CICS Transaction Gateway\classes\ctgclient.jar;". This path must be the same location that the monitored CTG client application uses.
   e. Configure the CTG CA SYSVIEW Agent:
      Copy the contents of the configuration template file Cross-Enterprise_APM_CTG_Config_Template.profile in the <Agent_Home>\wily\core\config directory into the IntroscopeAgent.profile file in the <Agent_Home>\wily\core\config directory. The template contains directions on how to use these additional configuration options. The options allow you to specify whether your installation supports CTG channels, and the transactions to be traced by matching on the program.
   f. Restart the CTG-based client application that the Java agent monitors. The client application can itself be an application server.
4. Enable the web services CA SYSVIEW tracer:
   
a. Install the SOA Performance Management tracer in
   &lt;Agent_Home&gt;\wily\examples\SOAPerformanceManagement by copying all files in the &lt;ext directory to the &lt;Agent_Home&gt;\wily\core\ext directory.

   **Note:** For more information, see the *CA Application Performance Management for SOA Implementation Guide*.

   b. Copy the ext\com.wily.introscope.ext.sysview.agent_&lt;version&gt;.jar and ext\WS-SYSVIEW-Tracer.jar files from the &lt;Agent_Home&gt;\wily\examples\Cross-Enterprise_APM\ext directory to the existing &lt;Agent_Home&gt;\wily\core\ext directory of the Introscope agent.

   c. Verify that the WS-SYSVIEW-Tracer.jar and com.wily.introscope.ext.sysview.agent_&lt;version&gt;.jar files are in the &lt;Agent_Home&gt;\wily\core\ext directory.

   d. Verify that the WS_Tracer_For_SYSVIEW.pbd file is in the &lt;Agent_Home&gt;\wily\core\config directory.

   e. Make the following edits to the IntroscopeAgent.profile file in the &lt;Agent_Home&gt;\wily\core\config directory:

   - Append spm.pbl and WS_Tracer_For_SYSVIEW.pbd to the introscope.autoprobe.directives property.
     
     For example:
     
     introscope.autoprobe.directivesFile=websphere-typical.pbl, hotdeploy, spm.pbl, WS_Tracer_For_SYSVIEW.pbd

   - Edit &lt;EM hostname&gt; to point to the Enterprise Manager computer.
     
     For example:
     
     introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=&lt;EM hostname&gt;

   f. Restart the web services client application that the Java agent monitors. The client application can itself be an application server.
5. Enable the HTTP CA SYSVIEW tracer:
   a. Copy the ext\com.wily.introscope.ext.sysview.agent_<version>.jar and ext\http-tracer.jar files from the <Agent_Home>\wily\examples\Cross-Enterprise_APM\ext directory to the existing <Agent_Home>\wily\core\ext directory of the Introscope agent.
   b. Verify that the http-tracer.jar and com.wily.introscope.ext.sysview.agent_<version>.jar files are in the <Agent_Home>\wily\core\ext directory.
   c. Verify that the HTTP_Tracer_For_SYSVIEW.pbd file is in the <Agent_Home>\wily\core\config directory.
   d. Make the following edits to the IntroscopeAgent.profile file in the <Agent_Home>\wily\core\config directory:
      ■ Append HTTP_Tracer_For_SYSVIEW.pbd to the introscope.autoprobe.directives property.
      For example:
      introscope.autoprobe.directivesFile=websphere-typical.pbl, hotdeploy, spm.pbl,HTTP_Tracer_For_SYSVIEW.pbd
      ■ Edit <EM hostname> to point to the Enterprise Manager computer.
      For example:
      introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=<EM hostname>
   e. Restart the web services client application that the Java agent monitors. The client application can itself be an application server.

Java Agent Component Files

The following table lists all the Java agent component files for the CA APM Cross-Enterprise.

<table>
<thead>
<tr>
<th>File</th>
<th>Directory Structure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS_Tracer_For_SYSVIEW.pbd</td>
<td>&lt;Agent_Home&gt;\wily\core\config</td>
<td>Required .PBD file for web services SYSVIEW tracer.</td>
</tr>
<tr>
<td>WS_Tracer_For_SYSVIEW-legacy.pbd</td>
<td>&lt;Agent_Home&gt;\wily\example\legacy</td>
<td>Required .PBD file for web services SYSVIEW tracer. Uses legacy version agent. Copy this file to &lt;Agent_Home&gt;\wily\core\config and use it instead of WS_Tracer_For_SYSVIEW.pbd if you want to run in legacy mode.</td>
</tr>
</tbody>
</table>
### File Directory Structure Description

<table>
<thead>
<tr>
<th>File</th>
<th>Directory Structure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WS-SYSVIEW-Tracer.jar</strong></td>
<td><code>&lt;Agent_Home&gt;/wily/examples/Cross-Enterprise_APM/ext</code></td>
<td>Required .JAR file.</td>
</tr>
<tr>
<td><strong>CTG_ECI_Tracer_For_SYSVIEW.pbd</strong></td>
<td><code>&lt;Agent_Home&gt;/wily/core/config</code></td>
<td>Required .PBD file for CTGtracer. Uses lean agent.</td>
</tr>
<tr>
<td><strong>CTG_ECI_Tracer_For_SYSVIEW-legacy.pbd</strong></td>
<td><code>&lt;Agent_Home&gt;/wily/examples/legacy</code></td>
<td>Required .PBD file for CTGtracer. Uses legacy version agent. Copy this file to <code>&lt;Agent_Home&gt;/wily/core/config</code> and use it instead of <code>CTG_ECI_Tracer_For_SYSVIEW.pbd</code> if you want to run in legacy mode.</td>
</tr>
<tr>
<td><strong>ctg-tracer.jar</strong></td>
<td><code>&lt;Agent_Home&gt;/wily/examples/Cross-Enterprise_APM/ext</code></td>
<td>Required .JAR file.</td>
</tr>
<tr>
<td><strong>HTTP_Tracer_For_SYSVIEW.pbd</strong></td>
<td><code>&lt;Agent_Home&gt;/wily/core/config</code></td>
<td>Required .PBD file for http-tracer. Uses lean agent.</td>
</tr>
<tr>
<td><strong>HTTP_Tracer_For_SYSVIEW-legacy.pbd</strong></td>
<td><code>&lt;Agent_Home&gt;/wily/examples/legacy</code></td>
<td>Required .PBD file for http-tracer. Uses legacy version agent. Copy this file to <code>&lt;Agent_Home&gt;/wily/core/config</code> and use it instead of <code>HTTP_Tracer_For_SYSVIEW.pbd</code> if you want to run in legacy mode.</td>
</tr>
<tr>
<td><strong>com.wily.introscope.ext.sysview.agent_&lt;version&gt;.jar</strong></td>
<td><code>&lt;Agent_Home&gt;/wily/examples/Cross-Enterprise_APM/ext</code></td>
<td>Required .JAR file.</td>
</tr>
<tr>
<td><strong>http-tracer.jar</strong></td>
<td><code>&lt;Agent_Home&gt;/wily/examples/Cross-Enterprise_APM/ext</code></td>
<td>Required .JAR file.</td>
</tr>
</tbody>
</table>

### Running with Legacy Mode PBDS

You can run with legacy versions of the PBDS instead of the new mode versions that are already placed in the directory `<Agent_Home>/wily/core/config`.

**Follow these steps:**

1. Select and run the Java agent installer for your environment.

   **Note:** For more information on legacy mode pbds, see the CA APM Java Agent Implementation Guide.

   After you run the installer, verify that these files are in the following directories:
   - `<Agent_Home>/wily/examples/legacy/CTG_ECI_Tracer_For_SYSVIEW-legacy.pbd`
   - `<Agent_Home>/wily/examples/legacy/WS_Tracer_For_SYSVIEW-legacy.pbd`
   - `<Agent_Home>/wily/examples/legacy/HTTP_Tracer_For_SYSVIEW-legacy.pbd`
2. Enable the legacy CTG CA SYSVIEW tracer by doing the following:
   a. Copy the CTG_ECI_Tracer_For_SYSVIEW-legacy.pbd from the 
      `<Agent_Home>\wily\examples\legacy` directory to the Introscope agent’s 
      existing `<Agent_Home>\wily\core\config` directory.
   b. Copy com.wily.introscope.ext.sysview.agent <version>.jar and ctg-tracer.jar 
      files from the `<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext` 
      directory to the Introscope agent’s existing `<Agent_Home>\wily\core\ext` 
      directory.
   c. Verify that ctg-tracer.jar and com.wily.introscope.ext.sysview.agent 
      <version>.jar files are located in the `<Agent_Home>\wily\core\ext` directory.
   d. Make the following edits:
      - Append CTG_ECI_Tracer_For_SYSVIEW-legacy.pbd to the 
        introscope.autoprobe.directives property. For example:
          introscope.autoprobe.directivesFile=CTG_ECI_Tracer_For_SYSVIEW-legacy.pbd
          hotdeploy
      - Edit `<EM hostname>` to point to the Enterprise Manager computer. For 
        example:
        introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=<EM
        hostname>
   e. Add the ctgclient.jar file to the classpath. For example, 'C:\Program
      Files\IBM\CICS Transaction Gateway\classes\ctgclient.jar;'. This path must be 
      the same location that the monitored CTG client application uses.
   f. Further configure the CTG CA SYSVIEW Tracer by copying the contents of the 
      configuration template file 
      `Cross-Enterprise_APM_CTG_Config_Template.profile` in the 
      `<Agent_Home>\wily\core\config` directory into the IntroscopeAgent.profile file 
      in the `<Agent_Home>\wily\core\config` directory. There are directions in the 
      template on how to use these additional configuration options which allow you 
      to specify whether your installation supports CTG channels, and the 
      transactions that should be traced by matching on the program.
   g. Restart the CTG-based legacy client application that the Java agent monitors. 
      The client application may itself be an application server.

3. Enable the legacy web services CA SYSVIEW tracer by doing the following:
   a. Copy the WS_Tracer_For_SYSVIEW-legacy.pbd from the 
      `<Agent_Home>\wily\examples\legacy` directory to the Introscope agent’s 
      existing `<Agent_Home>\wily\core\config` directory.
   b. Install the SOA Performance Management tracer located in 
      `<Agent_Home>\wily\examples\SOAPerformanceManagement` by copying all 
      files in the ext directory to the `<Agent_Home>\wily\core\ext` directory.
      **Note:** For more information, see the CA APM for SOA Implementation Guide.
      Please install the legacy version of the SOA tracer.
c. Copy the ext\com.wily.introscope.ext.sysview.agent_<version>.jar and ext\WS-SYSVIEW-Tracer.jar files from the
<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext directory to the
Introscope agent’s existing <Agent_Home>\wily\core\ext directory.
d. Verify that the WS-SYSVIEW-Tracer.jar and
com.wily.introscope.ext.sysview.agent_<version>.jar files are in the
<Agent_Home>\wily\core\ext directory.
e. Verify that the WS_Tracer_For_SYSVIEW-legacy.pbd file is in the
<Agent_Home>\wily\core\config directory.
f. Make the following edits to the IntroscopeAgent.profile file in the
<Agent_Home>\wily\core\config directory:
   ■ Append WS_Tracer_For_SYSVIEW-legacy.pbd to the
     introscope.autoprobe.directives property. For example:
     introscope.autoprobe.directivesFile=websphere-typical.pbl, hotdeploy,
     spm.pbl, WS_Tracer_For_SYSVIEW-legacy.pbd
   ■ Edit <EM hostname> to point to the Enterprise Manager computer. For
     example:
     introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT=<EM
     hostname>
g. Restart the web services client application that the Java agent monitors. The
client application may itself be an application server.

4. Enable the legacy HTTP CA SYSVIEW tracer by doing the following:
a. Copy the HTTP_Tracer_For_SYSVIEW-legacy.pbd from the
<Agent_Home>\wily\examples\legacy directory to the Introscope agent’s
existing <Agent_Home>\wily\core\config directory.
b. Copy the ext\com.wily.introscope.ext.sysview.agent_<version>.jar and
ext\http-tracer.jar files from the
<Agent_Home>\wily\examples\Cross-Enterprise_APM\ext directory to the
Introscope agent’s existing <Agent_Home>\wily\core\ext directory.
c. Verify that the com.wily.introscope.ext.sysview.agent_<version>.jar and
http-tracer.jar files are located in the <Agent_Home>\wily\core\ext directory.
d. Verify that the HTTP_Tracer_For_SYSVIEW-legacy.pbd file is in the
<Agent_Home>\wily\core\config directory. Make the following edits to the
IntroscopeAgent.profile file in the <Agent_Home>\wily\core\config directory:

- Append HTTP_Tracer_For_SYSVIEW-legacy.pbd to the
  introscope.autoprobe.directives property. For example:
  introscope.autoprobe.directivesFile=HTTP_Tracer_For_SYSVIEW.pbd,hotdeploy
- Edit <EM hostname> to point to the Enterprise Manager computer. For
  example:
  introscope.agent.enterprise.manager.transport.tcp.host.DEFAULT=<EM
  hostname>

e. Restart the HTTP-based client application that the Java agent monitors. The
  client application may itself be an application server.

Uninstall the Java Agent Component Files

If you choose to uninstall the Java agent component files, perform these steps.

Follow these steps:

1. Stop the agent.
2. Edit the IntroscopeAgent.profile file in the wily directory by removing these entries
   from the introscope.autoprobe.directives property.
   - WS_Tracer_For_SYSVIEW.pbd (or the legacy version)
   - CTG_ECI_Tracer_For_SYSVIEW.pbd (or the legacy version)
   - HTTP_Tracer_For_SYSVIEW.pbd (or the legacy version)
3. Remove any files copied from
   <Agent_Home>\wily\examples\Cross-Enterprise_APM that are in the
   <Agent_Home>\wily\core\ext directory.
4. Restart the agent to apply the changes.

Install the MQ Tracer (Optional)

This step is optional on the front-end Java application. Perform the following tasks only
if your front-end application is invoking CICS transactions using MQ.

If you use MQ tracer, you have the following options:

- Install the MQPowerPack tracer only if you want to trace the MQ application on the
  frontend application server and CICS.
- Install all the MQPowerPack if you also want to trace message flow through MQ.

To install the MQ tracer, follow the instructions provided in the CA APM for IBM
WebSphere MQ documentation for all MQ installation-related content.
Install and Configure the CA APM Cross-Enterprise Agent

Install the CA APM Cross-Enterprise Agent using one of the various methods available. After you have installed the extension, deploy, and configure it.

Install the CA APM Cross-Enterprise Agent using System Modification Program/Extended (SMP/E). SMP/E is the standard installation tool for managing operating system components and middleware on z/OS.

You can use any one of the following three methods to install the CA APM Cross-Enterprise product: SMP/E CA Chorus Software Manager (CA CSM), ESD, or tape. CA Chorus Software Manager (CA CSM) is the preferred method, because it is the easiest. However, if you do not have it, electronic software delivery (ESD) would be the recommended method. If you cannot install an electronic copy, you can use tape.

Install Using CA Chorus Software Manager

For more information about installing using CA Chorus Software Manager, see the CA Chorus Software Manager Installation Guide.

Note: If you install CA APM Cross-Enterprise using CA CSM, you must deploy the CA APM Cross-Enterprise Agent. For more information, see Deploy the Cross-Enterprise APM Agent (see page 31).

How to Install a Product Using Pax-Enhanced ESD

If you can install electronic software copies, you can use this method.

Follow these steps:

1. Download the 4000007C400.pax.Z file (listed as CA APM Cross-Enterprise EXT Z/OS-ESD) from the CA APM software download area on CA Support into the USS path of your choosing.

2. Unpax the ESD file /path/4000007C400.pax.Z into directory /path/4000007C400 using the following sample batch JCL:

```bash
//userid JOB (account#),CLASS=a,MSGCLASS=x  <<< Customise JOB card
//         SET PATH='/path'  <<< Customise install path
//UNPAXDIR EXEC PGM=BPXBATCH,
    // PARM=’sh cd &PATH; pax -rvf 4000007C400.pax.Z’
//STDOUT DD SYSOUT=*  
//STDERR DD SYSOUT=*
```
3. Customize the sample batch JCL in file `/path/4000007C400/UNZIPJCL` as instructed.

4. Submit the batch job to unzip the unpaxed files into MVS data sets that will be named using the high level qualifier (`yourHLQ`) that you specify in the JCL.

5. Customize the sample batch JCL in member `yourHLQ.CAI.SAMPJCL(SMPALLOCl)` as instructed.

6. Submit the batch job to allocate and mount the z/FS file system and MVS data sets required for installation.
   The MVS data sets will be named using the high level qualifier (`smp`) specified in the JCL and the z/FS file system will be mounted on the mount point `/root/C7C4960/`, using the root name specified in the JCL. The default value for root is `/usr/lpp/CAI`.

7. Carefully read the CA EULA in the `yourHLQ.CAI.SMPMCS` data set in SMP/E HOLDDATA.

8. Customize the sample batch JCL in member `yourHLQ.CAI.SAMPJCL(SMPINSDA)` as instructed.

9. BYPASS the SMP/E HOLDDATA that contains the CA End User License Agreement.
   This confirms that you have read, understood, and will comply with all the terms and conditions outlined in the EULA.

10. Submit the batch job to SMP/E RECEIVE, APPLY, and ACCEPT the CA APM Cross-Enterprise base product into the SMP/E target library `smp.C7C4JCL` and SMP/E target paths `/root/C7C4960/C7C4HFS/` and `/root/C7C4960/C7C4JAR/`.

11. After you have finished installing the extension, deploy it. For more information, see Deploy the Cross-Enterprise APM Agent (see page 31).

### How to Install a Product Using Tape

If you cannot install electronic copies of the software, you can use tape to install the extension.

**Follow these steps:**

1. Download the `CAI.SAMPJCL` library from file #1 of the CA APM Cross-Enterprise distribution tape into the MVS data set `yourHLQ.SAMPJCL` and specify the high-level qualifier (`yourHLQ`) of the MVS data set name using the following sample batch JCL:

   ```
   //userid    JOB (account#),CLASS=a,MSGCLASS=x  <<< Customize JOB card
   //         SET DISKPFX='yourHLQ.',' <<< Customize dname prefix
   //         SET DISKVOL='yourvol'  <<< Customize dsn volume
   //         SET TAPEUNIT='3480'   <<< Customize tape UNIT
   //         SET TAPEVOL='SYWC50'
   ```
Install and Configure the CA APM Cross-Enterprise Agent

//COPYJCL EXEC PGM=IEBCOPY
//SYSUT1 DD DISP=OLD,DSN=CAI.SAMPJCL,
//       LABEL=(1,SL),
//       UNIT=STAPEUNIT,
//       VOL=SER=STAPEVOL
//SYSUT2 DD DISP=(,CATLG),DSN=DISKPFX.SAMPJCL,
//       VOL=SER=DISKVOL,
//       SPACE=(TRK, (5,5,10)),
//       DCB=(RECFM=FB,LRECL=80,BLKSIZE=27920)
//SYSUT3 DD UNIT=VIO,SPACE=(CYL, (1,1))
//SYSUT4 DD UNIT=VIO,SPACE=(CYL, (1,1))
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COPY INDD=SYSUT1,OUTDD=SYSUT2

2. Customize the sample batch JCL in member yourHLQ.SAMPJCL(SMPALLOC) as instructed.

3. Submit the batch job to allocate and mount the z/FS file system and MVS libraries required for installation.
   The MVS data sets will be named using the high level qualifier (smp) that you specify in the JCL and the z/FS file system will be mounted on the mount point /root/C7C4960/, using the root name that you specify in the JCL. The default value for root is /usr/lpp/CAI.

4. Customize the sample batch JCL in member yourHLQ.SAMPJCL(SMPRCVTA) as instructed.

5. Submit the batch job to SMP/E RECEIVE the CA APM Cross-Enterprise base product into the SMP/E CSI smp.CSI.

6. Carefully read the CA EULA in the SMPRPT SYSOUT data set in SMP/E HOLDDATA.

7. Customize the sample batch JCL in member yourHLQ.SAMPJCL(SMPINSTA) as instructed.

8. BYPASS the SMP/E HOLDDATA that contains the CA End User License Agreement.
   This confirms that you have read, understood, and will comply with all the terms and conditions outlined in the EULA.

9. Submit the batch job to SMP/E APPLY and ACCEPT the CA Wily Extension for CA SYSVIEW base product into the SMP/E target library smp.C7C4JCL and SMP/E target paths /root/C7C4960/C7C4HFS/ and /root/C7C4960/C7C4JAR/.

10. Check for the latest service pack PTF and apply it using SMP/E according to the directions with the PTF.

11. After you have finished installing the extension, deploy it. For more information, see Deploy the Cross-Enterprise APM Agent (see page 31).
Install and Configure the CA APM Cross-Enterprise Agent

Deploy the CA APM Cross-Enterprise Agent

After you have installed the extension using the method that you prefer, deploy it.

Follow these steps:

1. Using ISPF View, customize the sample batch JCL in member `smp.C7C4JCL(COPYSAMP)` as instructed in the sample JCL.
   
   **Note:** Before you continue with the next step, be aware that your customized job `smp.C7C4JCL(COPYSAMP)` is not saved. Back it up if it is necessary.

2. Submit the batch job.

   The job makes a copy of data set `smp.C7C4JCL` that you customize for your site.

   This customized data set is named `custom.JCL`, using the high-level qualifier (`custom`) specified in the JCL. Additionally, the contents of SMP/E Target data set, `smp.C7C4JCL`, are copied into the customizable data set `custom.JCL`, which includes these members:

   - COPYSAMP
   - DEPLOY
   - START
   - STDENV
   - STOP
   - WILYZOS

3. Customize the sample batch JCL member in `custom.JCL(DEPLOY)` as instructed in the sample JCL.

4. Submit the batch job.

   The job deploys (copies) the contents of your installed SMP/E target paths `/root/C7C4960/C7C4HFS` and `/root/C7C4960/C7C4JAR` into the run-time path `/root/C7C4960/Cross-Enterprise_APM/`.

5. Customize the sample CA APM Cross-Enterprise startup JCL PROC in the `custom.JCL(WILYZOS)` member as instructed inside that JCL, specifying your `/root/C7C4960 z/FS` file system mount point.

   **Important!** If the CA SYSVIEW CNM4BLOD data set is not in the system linklist, uncomment the corresponding STEPLIB statement.

6. Copy the member into a standard PROCLIB defined on your system, such as `SYS1.PROCLIB`. 
7. Edit these variables in `custom.JCL(STDENV)`:  
   - Set the SA_INSTALL variable to the actual Cross-Enterprise_APM installation path.
   - Set the SYSVIEWPATH variable to the actual path of the CA SYSVIEW release-specific directory.
   - Set the IRRRACFPATH variable to the actual path of the directory containing the IRRRacf.jar file (PassTicket support).
   - Set the JAVA_HOME variable to the installation path of the JRE.
   - Set the LIBPATH variable to include the directory containing the libIRRacf.so library (PassTicket support).
   - Set the TZ="EST5EDT" export the TZ environment variable which specifies the time zone.

8. Save the member.

### CA APM Cross-Enterprise Files

The following table lists all the extracted files.

<table>
<thead>
<tr>
<th>File</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introscope_Cross-Enterprise_</td>
<td>/root/C7C4960/Cross-Enterprise_APM/config</td>
<td>Used to specify Introscope specific information.</td>
</tr>
<tr>
<td>APM.profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cross-Enterprise_APM_Dynamic</td>
<td>/root/C7C4960/Cross-Enterprise_APM/config</td>
<td>Used to configure CA APM Cross-Enterprise properties</td>
</tr>
<tr>
<td>properties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYSVIEWMetrics.xml</td>
<td>/root/C7C4960/Cross-Enterprise_APM/data</td>
<td>Configuration file that includes list of metrics to be collected from CA SYSVIEW and commands to get them (internal use only).</td>
</tr>
<tr>
<td>EULA.txt</td>
<td>/root/C7C4960/Cross-Enterprise_APM/data</td>
<td>End user license agreement that needs to be read and agreed to.</td>
</tr>
<tr>
<td>EULAInstructions.txt</td>
<td>/root/C7C4960/Cross-Enterprise_APM/data</td>
<td>A file containing instructions that are printed to the log when the product is started but the EULA has not yet been accepted. The instructions tell how to accept the EULA.</td>
</tr>
<tr>
<td>File</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InsightMetrics.xml</td>
<td>/root/C7C4960/Cross-Enterprise_APM/data</td>
<td>Configuration file that includes the list of metrics to be collected from CA Insight DPM and the queries used to retrieve them (internal use only).</td>
</tr>
<tr>
<td>IntroscopeCAPIConfig.xml</td>
<td>/root/C7C4960/Cross-Enterprise_APM/data</td>
<td>Required agent file (internal use only).</td>
</tr>
<tr>
<td>SMFRecords255C27.conf</td>
<td>/root/C7C4960/Cross-Enterprise_APM/data</td>
<td>SMF Records Definition File (internal use only).</td>
</tr>
<tr>
<td>SMFSend255C27.reqs</td>
<td>/root/C7C4960/Cross-Enterprise_APM/data</td>
<td>SMF Send Metrics Requests file (internal use only).</td>
</tr>
<tr>
<td>XnetErrors.xml</td>
<td>/root/C&amp;C4960/Cross-Enterprise_APM/data</td>
<td>Configuration file used to define actions taken in response to error conditions (internal use only).</td>
</tr>
<tr>
<td>com.wily.introscope.ext.sysview.agent_&lt;version&gt;.jar</td>
<td>/root/C7C4960/Cross-Enterprise_APM/ext</td>
<td>CA Introscope® agent plug-in for CA SYSVIEW.</td>
</tr>
<tr>
<td>Agent.jar</td>
<td>/root/C7C4960/Cross-Enterprise_APM/lib</td>
<td>Required library files.</td>
</tr>
<tr>
<td>castor-1.0.4.jar</td>
<td>/root/C7C4960/Cross-Enterprise_APM/lib</td>
<td>Required library files.</td>
</tr>
<tr>
<td>commons-logging-1.0.4.jar</td>
<td>/root/C7C4960/Cross-Enterprise_APM/lib</td>
<td>Required library files.</td>
</tr>
<tr>
<td>log4j-1.2.14.jar</td>
<td>/root/C7C4960/Cross-Enterprise_APM/lib</td>
<td>Required library files.</td>
</tr>
<tr>
<td>Cross-Enterprise_APM.jar</td>
<td>/root/C7C4960/Cross-Enterprise_APM/lib</td>
<td>Required library files.</td>
</tr>
<tr>
<td>Cross-Enterprise_APM.log</td>
<td>/root/C7C4960/Cross-Enterprise_APM/logs</td>
<td>Log file for Cross-Enterprise APM.</td>
</tr>
<tr>
<td>WILYZOS.sh</td>
<td>/root/C7C4960/Cross-Enterprise_APM/</td>
<td>Script used to start or stop agent.</td>
</tr>
<tr>
<td>WILYZOS</td>
<td>custom.JCL</td>
<td>Job control language to start and stop the agent.</td>
</tr>
</tbody>
</table>

**Note:** This shell script is necessary only if you run the Agent from USS. However, it is highly recommended to run the Agent from the JCL.
Configure the CA APM Cross-Enterprise Agent

This diagram provides a high-level overview of the CA APM Cross-Enterprise Agent configuration steps.

Before you begin

Before you begin configuring the CA APM Cross-Enterprise Agent, verify that you have Set Up CAICCI for CA APM Cross-Enterprise (see page 13).
**Follow these steps:**

1. Collect the metrics from CA SYSVIEW by configuring the CA APM Cross-Enterprise Agent. Establish a session with the CA SYSVIEW user address space by setting these configurations:
   
a. Configure the SYSVIEWPATH statement in custom.JCL(STDENV). Point the statement to the zFS directory that is created during the CA SYSVIEW SMP/E process, for example:

   ```
   SYSVIEWPATH=/usr/lpp/sysview/cnm4d70
   ```

   **Note:** Your directory varies according to the CA SYSVIEW release. Verify that the file being referenced in STDENV resides at the path you provide here.

   b. Configure the Cross-Enterprise_APM_Dynamic.properties file:

   ```
   SYSVIEW.connection.jobname=
   ```

   **Note:** The jobname parameter is not required because the agent discovers the CA SYSVIEW user address space running on the same system. This parameter is required only if you run multiple copies of CA SYSVIEW and multiple user address spaces.

   **Note:** For more information about setting the Cross-Enterprise_APM_Dynamic.properties configurations, see Configure the Cross-Enterprise_APM_Dynamic.properties File (see page 38).

2. Configure CA SYSVIEW to send the trace information to CA APM Cross-Enterprise.

   a. Establish a TCP listener to which the CA SYSVIEW CICS and IMS loggers connect. The configuration is set by editing this property in the Introscope_Cross-Enterprise_APM.profile file:

   ```
   ppz.smf.socket.port=15029
   ```

   b. Connect the CICS logger and IMS logger tasks in the CA SYSVIEW server to the CA APM Cross-Enterprise TCP listener on the specified port. Edit the following properties in the CA SYSVIEW data members:

   ```
   sysvhql.CNM4BPRM(CICSLOGR)
   Wily-Introscope-PortList CICSWILY

   sysvhql.CNM4BPRM(GROUPS)
   DEFINE CICSWILY
   TYPE PORTLIST
   DESC 'Wily Agent Listener Port'
   MEMBERS 15029

   sysvhql.CNM4BPRM(IMSLOGR)
   Wily-Introscope-PortList IMSWILY
   ```
sysvhlq.CNM4BPRM(GROUPS)
DEFINE IMSWILY
    TYPE PORTLIST
    DESC 'Wily Agent Listener Port'
    MEMBERS 15029

Note: For more information about setting the Introscope_Cross-Enterprise_APM.profile configurations, see Configure the Introscope_Cross-Enterprise_APM.profile File (see page 42).

Note: After you configure these settings, read and accept the End User License Agreement. For more information, see Configure and accept the End User License Agreement (see page 37).

About the CA APM Cross-Enterprise Configuration Files

The CA APM Cross-Enterprise can be customized to fit your operating environment by setting various properties in the configuration files to meet your needs.

<table>
<thead>
<tr>
<th>File</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-Enterprise_APM_Dynamic.properties</td>
<td>/root/C7C4960/Cross-Enterprise_APM/config</td>
<td>The main CA APM Cross-Enterprise configuration file. This file is where the major extension-related features are configured.</td>
</tr>
<tr>
<td>Introscope_Cross-Enterprise_APM.profile</td>
<td>/root/C7C4960/Cross-Enterprise_APM/config</td>
<td>The standard CA Introscope agent configuration file that provides all required properties to connect and communicate to CA Introscope Enterprise Manager.</td>
</tr>
<tr>
<td>STDENV</td>
<td>custom.JCL</td>
<td>The shell script containing the main configuration variables for running the agent PROC.</td>
</tr>
</tbody>
</table>
Configure and Accept the End User License Agreement

Read and accept the end user license agreement.

**Important!** If you do not acknowledge the license agreement, error message WILY004E displays.

**Follow these steps:**

1. Open the EULA.txt file at `/root/C7C4960/Cross-Enterprise_APM/data`, and read the terms.
2. After you have agreed to the terms, open the `Cross-Enterprise_APM_Dynamic.properties` file at `/root/C7C4960/Cross-Enterprise_APM/config` and set the following property:

   ```
   ```

3. Save the file.

   The accepted agreement is applied after the agent is restarted.

Configure Network Topology and Firewall Settings

Open firewall ports between CA APM Cross-Enterprise and the Enterprise Manager to allow them to communicate. To allow the bi-direction communication between all appropriate Enterprise Managers and the CA APM Cross-Enterprise Agent, update the firewall in both directions.

In a clustered environment, an Enterprise Manager serves as a Manager of Managers (MOM), managing the other Enterprise Managers in the cluster (named Collectors). For load-balancing, the Introscope agents that connect to the MOM are redirected to a Collector with the lightest weight-adjusted load in the cluster. If an agent is disconnected later from the Collector, the agent reconnects to the MOM and can be assigned to a different Collector. In this MOM environment, configure the CA APM Cross-Enterprise Agent to connect directly to MOM or directly specify an Enterprise Manager.

**Follow these steps:**

1. Open the Introscope_Cross-Enterprise_APM.profile file at `/root/C7C4960/Cross-Enterprise_APM/config`.
2. Edit the `introscope.agent.enterprisemanager.transport.tcp.port.DEFAULT=5001` property if you want to use an Enterprise Manager connection port other than the 5001 default port.
Install and Configure the CA APM Cross-Enterprise Agent

**Note:** If it is a MOM environment with load balancing and the CA APM Cross-Enterprise Agent is configured to connect to a MOM, then the Enterprise Manager connection port to this MOM and all Collectors that are defined to the MOM must be opened in the firewall. The Enterprise Manager connection port for the Collector is defined in the `<agent-Collector>` element of the `loadbalancing.xml` file on the MOM Enterprise Manager machine. For more information about configuring load balancing, see the *CA APM Configuration and Administration Guide*.

3. Restart the CA APM Cross-Enterprise Agent.
   The settings are applied.

4. Verify the connection between the CA APM Cross-Enterprise and the Enterprise Manager hosts in both directions by using the `ping` command.

**Configure the Cross-Enterprise_APM_Dynamic.properties File**

The *Cross-Enterprise_APM_Dynamic.properties* file is the main extension configuration file, in that it allows you to specify these settings for the CA APM Cross-Enterprise:

- Top worst performing transactions to retain
- Regular expression pattern to filter which CICS regions to monitor
- Regular expression pattern to filter which transaction groups to monitor
- Regular expression pattern to filter which queue managers to monitor
- Regular expression pattern to filter which queues to monitor
- Regular expression pattern to filter which IMS subsystems to monitor
- Regular expression pattern to filter which IMS transaction groups to monitor
- Regular expression pattern to filter which Datacom address spaces to monitor
- Regular expression pattern to filter which TCP/IP stacks to monitor
- Option to turn off collection of z/OS metrics
- Option to turn off collection of SYSVIEW metrics
- The format of the URL for the transaction trace click-through feature
- The frequency for which static metrics are reported
- The metric update interval for retrieving CA SYSVIEW metrics
- The parameters that are required to connect to a specific CA SYSVIEW
- The configuration options to turn off z/OS metric collection or metric collection completely
- The configuration options to allow distinct collection intervals for each metric category
The following configuration properties must be properly set to collect metrics from one or more CA Insight DPM for DB2 for z/OS agents running on the local LPAR:

- **Insight.metrics.collect** — This configuration parameter determines whether metrics are collected from any CA Insight DPM for DB2 for z/OS instance running on the local LPAR. If this parameter is set to no, then no DB2-specific metrics are collected. If this parameter is set to yes, the Cross-Enterprise APM Agent attempts to contact the configured XNET agent subtask of CA Insight DPM for DB2 for z/OS and retrieve DB2-specific metrics.

- **Insight.connection.port** — This configuration parameter allows you to specify the TCP/IP port that is used by the local XNET agent subtask of CA Insight DPM for DB2 for z/OS to listen for query requests. This XNET agent subtask must be enabled and configured for the Cross-Enterprise APM Agent to collect DB2-specific metrics.

- **Insight.passticket.support** — This configuration parameter determines whether to use PassTickets when sending authentication information to the XNET agent subtask of CA Insight DPM for DB2 for z/OS. In order to use PassTicket authentication, your active z/OS security manager must be properly configured to allow for PassTicket creation, the user account used to start the Cross-Enterprise APM Agent must have the proper permissions to create PassTickets, and the XNET agent subtask must be configured to allow for PassTicket authentication. If this parameter is set to yes, PassTickets are used for authentication instead of user passwords. If this parameter is set to no, you must specify a valid user password in the Insight.password configuration parameter.

- **Insight.passticket.app** — If the Insight.passticket.support parameter is set to yes, use this configuration parameter to specify the application name that is used to generate PassTicket authentication tokens. The XNET agent subtask of CA Insight DPM for DB2 for z/OS must be configured to use this application name by specifying the same value in the PASSNAME() configuration parameter.

- **Insight.username** — This configuration parameter is used to specify the user name sent to the XNET agent subtask of CA Insight DPM for DB2 for z/OS for authentication. This parameter must always be specified, regardless of whether PassTicket support is enabled.

- **Insight.password** — This configuration parameter is used to specify the user password sent to the XNET agent subtask of CA Insight DPM for DB2 for z/OS for authentication. If PassTicket support is not enabled, this parameter must be specified. If PassTicket support is enabled, this parameter is required to remain blank. For security reasons, use PassTicket authentication to avoid storing unencrypted passwords in the configuration file.
- **Insight.DB2.subsystem.name.list** — This configuration parameter is used to specify which local DB2 instances the CA APM Cross-Enterprise Agent monitors. A connection is established to each data Collector instance of CA Insight DPM for DB2 for z/OS monitoring a DB2 subsystem that is specified in this comma-separated list. In order to collect metrics from all local CA Insight for DB2 for z/OS data Collector instances that are monitoring DB2 subsystems, specify the '*' wildcard character for this value of this parameter.

- The remaining configuration parameters that are listed in the Cross-Enterprise_APM_Dynamic.properties file that begin with the *Insight* prefix have default values that will function properly for most installations.

The following Insight configuration properties influence the collection performance of metrics from local DB2 subsystems:

- **Insight.DB2.subsystem.refresh.interval** — This configuration parameter is used to specify how often the Cross-Enterprise APM Agent both refreshes the list of accessible DB2 subsystems and submits status queries to each DB2 subsystem. The default value for this parameter is half of the Insight.update.interval parameter value. This default value should be adequate for most situations, but this parameter value can be changed if necessary. The default value is 60 seconds or half of the Insight update interval.

- **Insight.DB2.subsystem.refresh.threads** — This configuration parameter is used to specify how many operating system threads are used to process the tasks defined to run during the DB2 subsystem refresh interval. The default value for this parameter is 1, which means a single thread is used to issue status queries to each configured DB2 subsystem. If the DB2 subsystem refresh interval needs to execute quicker, the value for this configuration parameter can be increased to allow multiple tasks to execute simultaneously (at the cost of increased CPU consumption during the refresh interval).

- **Insight.update.interval** — This configuration parameter is used to specify how often the Cross-Enterprise APM Agent retrieves updated metric values from each configured DB2 subsystem. The default value for this parameter is the value defined for the SYSVIEW.update.interval parameter. The value of this configuration parameter can be increased, which will decrease the rate configured DB2 subsystems need to process metric value queries. The default value is 120 seconds.

- **Insight.update.threads** — This configuration parameter is used to specify how many operating system threads are used to process the metric value queries sent to each configured DB2 subsystem. The default value for this parameter is 1, which means the same thread is used to sequentially process each configured DB2 subsystem query. If the metric update interval needs to execute quicker, the value for this configuration parameter can be increased to allow multiple metric value queries to execute simultaneously (at the cost of increased CPU consumption during the metric update interval).

The properties file contains explicit detail, examples, and lists the configuration options available to help you choose what best suits your environment.
Follow these steps:

1. Open the `Cross-Enterprise_APM_Dynamic.properties` file, located at 
   `/root/C7C4960/Cross-Enterprise_APM/config`.
2. Edit and save the text file.
   The changes will be applied after they are picked up by the agent dynamically.

Use Groups to Filter Queue Managers and Queues

A way to reduce waste in processing power is to filter out unnecessary data before it reaches the CA APM Cross-Enterprise Agent. Include or exclude queue managers for the WILYQM group and queues for the WILYQUE group definition.

CA SYSVIEW automatically includes definitions for the WILYQM and WILYQUE groups. We recommend that you add members to these groups so that the agent receives only those queues that are related to the applications in use.

By default, CA SYSVIEW includes all queue managers and queues except for the temporary queues.

**Note:** You may find that you do not need all that data.

CA SYSVIEW automatically filters out the temporary queues, such as PERMDYN and TEMPDYN. You do not have to exclude these queues specifically from the group definitions.

Add a queue manager or queue to the group by adding a separate member key/value pair on a separate line.

**Group Definitions**

```plaintext
sysvhlq.CM4BPRM(GROUPS)

DEFINE WILYQM
    TYPE      MQQMGR
    DESC      'Wily monitored queue managers'
    MEMBER    =

DEFINE WILYQUE
    TYPE      MQQUEUE
    DESC      'Wily monitored queues'
    MEMBER    =
```
Example: Filter Queue Managers and Queues

This example shows how to exclude and include queue managers and queues in the group definitions. The modified group definitions exclude the XYZ queue manager and include the ABC queue.

```plaintext
DEFINE WILYQM
  TYPE  MQQMGR
  DESC  'Wily monitored queue managers'
  MEMBER =
  EXCLUDE  XYZ

DEFINE WILYQUE
  TYPE  MQQUEUE
  DESC  'Wily monitored queues'
  MEMBER =
  MEMBER    ABC
```

Configure the Introscope_Cross-Enterprise_APM.profile

The `Introscope_Cross-Enterprise_APM.profile` file is where the agent configuration required to communicate to Enterprise Manager and CA SYSVIEW agent are made.

Introscope_Cross-Enterprise_APM.profile is a standard CA Introscope® agent configuration file that provides all required properties to connect and communicate to Enterprise Manager. Any update in the file requires that you restart the CA APM Cross-Enterprise Agent.

In addition to other settings, you can set these CA SYSVIEW-related properties in this configuration file:

- Turn sampling on or off, and at interval collect such and such.
- Disable or enable the ability to acquire metrics.
- Specify the TCP/IP port so the SMF records can be obtained from CA SYSVIEW.
- Set the agent antiflood threshold, which specifies the number of traces that are sent to Enterprise Manager by the CA APM Cross-Enterprise Agent.
- Specify the amount of detail that is logged and the output location.
- If there are multiple IP stacks with different security permissions, specify the specific IP stack to bind the agent to.
The properties file contains explicit detail, examples, and lists the configuration options available to help you when configuring settings for your environment.

Follow these steps:
1. Open the Introscope_Cross-Enterprise_APM.profile file, which is at /root/C7C4960/Cross-Enterprise_APM/config.
2. Edit and save the text file.
3. Restart the CA APM Cross-Enterprise Agent.
   The settings are applied.

**Configure Transaction Sampling**

Transaction sampling enables CA Introscope® agents to take a transaction trace occasionally without having an explicit transaction trace session running. The sampling does not apply any filtering and wakes up on a timer to take the sample. The samples are visible from the Workstation.

**Important!** The sampled traces are only visible from the Workstation Investigator metric tree traces tab. The traces do not show in the Transaction Trace Viewer of a transaction trace session.

Trace samples that are taken from a front-end agent automatically attempt to generate correlated cross-process back-end transaction traces. Samples that are generated directly from the CA APM Cross-Enterprise Agent do not always have correlated front-end traces. For more information about Cross-Process Transaction Traces, see *About Cross-Process Transaction Traces* (see page 98).

Follow these steps:
1. Configure each front-end agent making the following edits to the IntroscopeAgent.profile file in the <Agent_Home>\wily\core\config directory.
2. Configure the CA APM Cross-Enterprise Agent by opening the Introscope_Cross-Enterprise_APM.profile file, at /root/C7C4960.
3. Edit these settings as required:
   - introscope.sysview.agent.transactiontracer.sampling.enabled
     This parameter enables or disables the transaction sampling. The default value is true. If this parameter is set to false, the other parameters are ignored.
**Install and Configure the CA APM Cross-Enterprise Agent**

- `intrascop.e.sysview.agent.transactiontracer.sampling.interval.seconds`
  This value specifies when the transaction sample is captured. The sampling interval can range from 1 second up to 300 seconds (5 minutes). The default value is 120 seconds.

- `intrascop.e.sysview.agent.transactiontracer.sampling.perinterval.count`
  This value specifies the number of samples that are captured in a transaction sampling interval. The number can range from 1 to 1000 and has a default value of 15 seconds.

4. After you restart the CA APM Cross-Enterprise, the new settings are applied.

   Any transaction trace types that you receive have Sampled in the Trace Type field of the Properties section at the bottom of the Trace View tab.

**Start the CA APM Cross-Enterprise Agent**

Issue the following MVS operator command to start the CA APM Cross-Enterprise Agent:

```
MVS S WILYZOS
```

or

```
MVS S WILYZOS, ACTION=START
```

**Stop the CA APM Cross-Enterprise Agent**

Issue one of the following MVS operator commands to stop the CA APM Cross-Enterprise Agent:

```
MVS P WILYZOS
```

or

```
MVS S WILYZOS, ACTION=STOP
```

**Maintain the CA APM Cross-Enterprise Agent**

CA APM Cross-Enterprise is maintained using SMP/E.

**Download CA APM Cross-Enterprise Maintenance**

Download SMP/E maintenance for CA APM Cross-Enterprise from [CA Technical Support site](CA_Technical_Support_site), either manually or using CA CSM.
SMP/E RECEIVE and APPLY

Use SMP/E RECEIVE and APPLY to download the maintenance into SMP/E target paths /root/C7C4960/C7C4HFS/ and /root/C7C4960/C7C4JAR/, using either CA CSM or standard SMP/E batch JCL.

Note: The deployed runtime path /root/C7C4960/Cross-Enterprise_APM/ is not altered by this step.

Deploy an Updated Version of the CA APM Cross-Enterprise Agent

While SMP/E is used to install the extension, deployment is required to create the executable runtime path. Likewise, SMP/E is used to maintain or update the agent, deployment is required to update the executable runtime path. If you update the agent, deploy it using the steps in this topic.

Follow these steps:

1. Shut down CA APM Cross-Enterprise Agent by issuing the following MVS operator command:
   
   MVS P WILYZOS

2. Submit the custom.JCL(DEPLOY) batch job.
   
   The job deploys or copies the contents of your installed SMP/E target paths /root/C7C4960/C7C4HFS and /root/C7C4960/C7C4JAR into the runtime path /root/C7C4960/Cross-Enterprise_APM/.

3. Restart CA APM Cross-Enterprise Agent by issuing the following MVS operator command:
   
   MVS S WILYZOS

Note: After initial deployment, subsequent executions of the custom.JCL(DEPLOY) job to deploy any maintenance does not alter the /root/C7C4960/Cross-Enterprise_APM/config runtime path. The path contains configurable files that you have customized. If these files require maintenance, that maintenance contains HOLDDATA. The HOLDDATA instructs you on how to update these files manually to deploy that maintenance.

SMP/E ACCEPT

You can permanently SMP/E accept the maintenance that has been applied.

Important! The accepted maintenance cannot be undone.

If the deployed maintenance is good, accept the applied maintenance into the SMP/E Distribution libraries smp.ASYWHFS and smp.ASYWJAR, using either CA CSM or batch JCL.
SMP/E RESTORE

You can reject the maintenance that has been applied but not accepted, using SMP/E RESTORE.

If the deployed maintenance is bad, restore the SMP/E Target paths /root/C7C4960/C7C4HFS and /root/C7C4960/C7C4JAR, using either CA CSM or batch JCL.

You then deploy (copy) the restored Target paths (see page 45) /root/C7C4960/C7C4HFS and /root/C7C4960/C7C4JAR into the runtime path /root/C7C4960/Cross-Enterprise_APM/.

Configure CA SYSVIEW

There are minimum configurations that need to occur on the CA SYSVIEW side. These configurations tie into and should be done when the CA APM Cross-Enterprise configurations are made. To see specific instructions on how to configure CA SYSVIEW, see step 2 in the Configure the Cross-Enterprise APM Agent (see page 34).

Important! Using CA-SYSVIEW 13.5 or older versions will disable certain features. The metrics, typeviews, and dashboards will be disabled for z/OS Alerts, z/OS Degradation Delay Analysis, z/OS Workload Manager Service Goals, CICS Alerts, and CICS Degradation Analysis.
Verify the Installation

After CA APM Cross-Enterprise has been successfully installed, launch Introscope and go to the Investigator. You will see the host name of the z/OS machine and will see active metrics under the CA APM Cross-Enterprise node and backend CICS traces:
Chapter 2: Integrate CA NetMaster NM for TCP/IP with CA Introscope®

This section contains the following topics:

How You Integrate CA NetMaster NM for TCP/IP with CA Introscope® (see page 49)
Performance Monitoring Metrics (see page 53)
Specify the Performance Monitoring Metrics to Send (see page 54)

How You Integrate CA NetMaster NM for TCP/IP with CA Introscope®

As an application administrator, you want CA Introscope® to see CA NetMaster NM for TCP/IP performance data. You have both products already installed in your environment. To enable the visibility, you configure the integration between CA NetMaster NM for TCP/IP and CA Introscope®.

Note: For information about how to install CA NetMaster NM for TCP/IP, see the CA NetMaster Network Management for TCP/IP Installation Guide. If you have the CA Cross-Enterprise APM license but not the CA NetMaster NM for TCP/IP license, see the CA NetMaster Network Management for TCP/IP Installation Guide (for CA APM Restricted License).

The following illustration provides an overview of the process:

The process has the following tasks:

1. Verify file locations (see page 50).
2. Configure EPAgent (see page 50).
3. Confirm the connectivity (see page 51) between CA NetMaster NM for TCP/IP and EPAgent.
4. Configure CA NetMaster NM for TCP/IP (see page 52).
5. Verify the integration (see page 53).
At the end of the process, you can use the following facilities to work with the network performance data:

- Workstation Console or WebView to view dashboards of network metrics
- Workstation Investigator to examine network metrics
- Reporting on the data

**Verify File Locations**

Two files contain CA NetMaster NM for TCP/IP dashboards, typeviews, and report templates. During the installation of Enterprise Manager, if you have selected the CA Cross-Enterprise Application Performance Management option, the installation process puts these files in the correct locations.

Verify that the following files are in the indicated directory:

- `<EM_Home>\config\modules\NetMasterAgent_Management_Module.jar`
- `<EM_Home>\ext\ddtv\NetMasterAgent.typeviewers.xml`

If the files are not there, copy them from the `<EM_Home>\examples\Cross-Enterprise_APM\` directory. Then, restart Enterprise Manager.

**Configure EPAgent**

You customize the EPAgent properties file. If you want to connect more than two CA NetMaster NM for TCP/IP regions, you require a dummy plug-in file.

**Follow these steps:**

1. Customize the `<EPAgent_Home>/epagent/IntroscopeEPAgent.properties` file:
   a. Verify that the following line is uncommented:
      ```
      introscope.epagent.config.networkDataPort=8000
      ```
   b. Record this Network Data Port number.
   c. Specify Mainframe for the `introscope.agent.customProcessName` property:
      ```
      introscope.agent.customProcessName=Mainframe
      ```
   d. Specify NetMasterAgent for the `introscope.agent.agentName` property:
      ```
      introscope.agent.agentName=NetMasterAgent
      ```
e. (Optional) If you want to connect more than two CA NetMaster NM for TCP/IP regions, add stateless plug-ins.

For example, the following lines cater for three regions:

```
introscope.epagent.plugins.stateless.names=ZOS1,ZOS2,ZOS3
introscope.epagent.stateless.ZOS1.command=<EPAgent_Home>/epagent/epaplugins/dummy_file
dummy_file
troscope.epagent.stateless.ZOS1.delayInSeconds=86400
introscope.epagent.stateless.ZOS2.command=<EPAgent_Home>/epagent/epaplugins/dummy_file
dummy_file
introscope.epagent.stateless.ZOS2.delayInSeconds=86400
introscope.epagent.stateless.ZOS3.command=<EPAgent_Home>/epagent/epaplugins/dummy_file
dummy_file
introscope.epagent.stateless.ZOS3.delayInSeconds=86400
```

`dummy_file` identifies the dummy plug-in file that you create in the next step. The file has the following name:

- (Linux) `name.scr`
- (Windows) `name.bat`

f. Save the customized file.

2. (Optional) If you want to connect more than two CA NetMaster NM for TCP/IP regions, create a dummy plug-in file.

- (Linux) In the `<EPAgent_Home>/epagent/epaplugins/` directory, create a `.scr` file with a single comment line:
  ```
  # This is a dummy EPA plug-in file
  ```
- (Windows) In the `<EPAgent_Home>/epagent/epaplugins/` directory, create a `.bat` file with a single comment line:
  ```
  :: This is a dummy EPA plug-in file
  ```

3. Start EPAgent.

CA Introscope® is ready to accept data from CA NetMaster NM for TCP/IP.

### Confirm the Connectivity

Confirm the connectivity between the CA NetMaster NM for TCP/IP region and EPAgent. If firewalls exist, these firewalls must permit TCP/IP traffic between an ephemeral port on the z/OS IP host for the region and EPAgent Network Data Port (default 8000).

**Follow these steps:**

1. Log on to the region.
2. Enter **CMD** at the Command prompt.
   The Command Entry panel appears.
3. Enter the following command to ping the IP address of EPAgent:
   PING em_ip_address
4. Review the response to verify that the region can reach EPAgent.

   **Important!** If the test fails, reconfigure your firewalls to permit connectivity.

### Configure CA NetMaster NM for TCP/IP

You configure CA NetMaster NM for TCP/IP to enable the region to feed performance data to CA Introscope®.

**Follow these steps:**

1. Verify that the TESTEXEC(RUNSYSIN) member for the region contains the following parameter:
   
   PPREF='PROD=APM'

   **Important!** If you update the member, restart both the region and the associated SOLVE Subsystem Interface (SSI).

2. Log on to the region.
3. Enter /PARMS at the Command prompt.
   
   A list of parameter groups appears.
4. Enter F APMEPAGENT.
   
   The command finds the parameter group that enables the data feed.
5. Enter B next to the parameter group.
6. Verify that the following fields have the indicated values:

   ```
   - APMEPAGENT - CA Introscope EPAgent -------------------------------
   | CA Introscope Environment Performance Agent:                     |
   | Enable EPAgent Client? ................. YES (Yes or No)            |
   | IP Addr/Host Name ... epa_ip_address                                |
   | EPAgent Network Data Port .............. 8000                      |
   ```

   **epa_ip_address**

   Identifies the IP address or host name of EPAgent.

   **Note:** If an update is required, press the F4 (Update) function key. After your changes, press F6 (Action) to apply the changes effective immediately in the region, then press F3 (File) to save the changes.

   The region is already feeding or starts to feed data to CA Introscope®.
Verify the Integration

The quickest way to verify a new metric feed is to open a Workstation Console and view the NetMaster dashboards. The first data points start to appear about 15 seconds after you apply the APMEPAGENT parameter group. (Some metrics, such as Top Applications, only appear after about 5 minutes.)

Follow these steps:
1. Start and log in to Workstation Console.
2. Select a NetMaster dashboard from the Dashboards drop-down list at the top.
3. Confirm that the dashboard shows network performance data.

CA NetMaster NM for TCP/IP is feeding data to CA Introscope®, and you can use Workstation to work with the data.

Performance Monitoring Metrics

After you familiarize yourself with the default metrics, you can consider sending the Performance Monitoring metrics.

A CA NetMaster NM for TCP/IP region monitors performance metrics for many physical and logical mainframe network resource types. The metric sample values come from various sources including IBM operating system functions, device management applications, packet flow analysis, and physical devices.

At regular fixed intervals from 5 through 60 minutes, the region takes samples of each monitored metric. Metric sample values are compared to thresholds, for alerting. The sample values are aggregated into hourly values, for baseline calculations and further reporting, but are not retained for long periods.

Note: For information about how to configure monitoring for an IP resource or node, see the CA NetMaster Network Management for TCP/IP Implementation Guide. For information about monitoring attributes, see the CA NetMaster Network Management for TCP/IP Administration Guide.

You can send these metrics to CA Introscope®, for example:
- To retain individual sample values in specialized metric storage, for longer than the region can keep them

For example, you want to keep months of interface throughput rates at small intervals. You use this data for verification with their link provider.
Specify the Performance Monitoring Metrics to Send

- To create dashboards combining complementary mainframe metrics from different sources
  
  For example, you want to combine stack network interface metrics with OSA or Cisco device performance metrics.

- To create dashboards for critical business services from CA NetMaster NM for TCP/IP, CA SYSVIEW, and CA Insight DPM metrics, with multiple service components visible on one place

Specify the Performance Monitoring Metrics to Send

The Workstation Investigator lists the Performance Monitoring metrics under the IP Resources metric category. You can configure the CA NetMaster NM for TCP/IP region to send these metrics to CA Introscope®.

**Note:** To configure the region to monitor a metric (or attribute), see the *CA NetMaster Network Management for TCP/IP Implementation Guide*.

**Follow these steps:**

1. Log on to the region.

2. Identify the attributes that are monitored for an IP resource or node, and if applicable, qualifier name:
   
   a. Enter /IPMON to access IP Resource Monitor or /IPNODE to access IP Node Monitor.

   b. Find the IP resource or node, and enter H next to it.
      
      A list of attributes appears.

   c. Find the required attributes, and note down the following information, including any special characters:
      
      - Resource class
      - Resource name
      - Attribute name
      - Qualifier name

   **Note:** Do not include attributes of the ENUM type. The region does not send this type of attributes to CA Introscope®.

   **Note:** To avoid metric explosions and other overheads, the region can send a maximum of 64 resource-qualifier-attribute combinations.
Specify the Performance Monitoring Metrics to Send

Chapter 2: Integrate CA NetMaster NM for TCP/IP with CA Introscope®

3. Specify the attributes:
   a. Enter /PARMS at the Command prompt.
      A list of parameter groups appears.
   b. Enter F APMEPAGENT.
      The command finds the parameter group that enables the data feed.
   c. Enter U next to the parameter group.
   d. Specify YES in the Performance Monitoring field.
   e. Press F8 (Forward).
      A panel appears for you to specify the attributes you want to send.
   f. Specify the resource-qualifier-attribute combinations that you noted in Step 2c in the indicated syntax, for example:
      - ASMON(IKED TCPIP11V-UDP(500)) AsBytesInByPort
      - APPNHPR(APPNHPR) RTPsARBRred
      - CSM(CSM NET) DataSpaceTotalInUse
      - EE(EE USILDA01.NMDCIP2) EEBytesByCP
      - IPNODE(NMDCIP3 FastEthernet0/0) CiscoifOutPkts
      - CIP(NMDCIP3 192.168.82.232) CLAWReadBlks
      - OSA(OSA-00 TCPIP99-P4) PriorityQueueStatus
      - STACK(TCPIP31 172.24.*) ConActiveByNet
      - VIPA(DVIPA CO31-TCP/IP) ConConnectsByStack
      **Note:** For more information, press F1 (Help).
   g. Press F4 (Save).
   h. Press F6 (Action).
      Your changes become effective immediately. The current metric feed connection stops; then a new metric feed connection starts, including the Performance Monitoring metrics. You can see the values of these metrics at CA Introscope® after the first sampling interval.
Chapter 3: How to use the Console to Identify Problems

This section contains the following topics:

About CA APM Cross-Enterprise Dashboards (see page 57)
CA APM Cross-Enterprise - Mainframe Health Overview Dashboard (see page 60)
z/OS System Health Dashboard (see page 62)
CICS Regions Health Dashboard (see page 64)
CICS Transaction Groups Details Dashboard (see page 65)
IMS Subsystems Health Dashboard (see page 67)
IMS Transaction Groups Health Dashboard (see page 69)
CA Datacom Address Spaces Health Dashboard (see page 70)
Queue Managers Health Dashboard (see page 71)
WebSphere MQ Queues Health Dashboard (see page 73)
TCP/IP Stacks Health Dashboard (see page 74)
DB2 z/OS Performance Overview Dashboard (see page 75)
DB2 z/OS Subsystem Information Dashboard (see page 77)
DB2 z/OS CPU Activity Dashboard (see page 78)
DB2 z/OS Buffer Pool Activity Dashboard (see page 81)
DB2 z/OS EDM Pool Activity Dashboard (see page 84)
DB2 z/OS Lock Activity Dashboard (see page 86)
DB2 z/OS Log Activity Dashboard (see page 88)
DB2 z/OS Workload Dashboard (see page 90)
DB2 z/OS More Information Dashboard (see page 93)

About CA APM Cross-Enterprise Dashboards

CA APM Cross-Enterprise provides a series of out-of-the-box dashboards that can be viewed in the console. The dashboards that are included:

CA APM Cross-Enterprise: Mainframe Health Overview

Provides general system status at a glance.

CA APM Cross-Enterprise: z/OS System Health

This dashboard displays key metrics to help identify problems with the health of the z/OS system.

CA APM Cross-Enterprise: CICS Regions Health

Displays the metrics that report on the health of the CICS regions.

CA APM Cross-Enterprise: CICS Transaction Groups Details

Displays the metrics that report CICS transaction groups details.
About CA APM Cross-Enterprise Dashboards

CA APM Cross-Enterprise: IMS Subsystems Health
Displays the metrics that report on the health of the IMS subsystems.

CA APM Cross-Enterprise: IMS Transaction Groups
Displays the metrics that report on the health of the IMS transaction groups.

CA APM Cross-Enterprise: DATACOM Address Spaces Health
Displays the metrics that report on the health of the DATACOM address spaces.

CA APM Cross-Enterprise: Websphere MQ Queue Managers Health
Displays the metrics that report on the health of the WebSphere MQ queue managers.

CA APM Cross-Enterprise: Websphere MQ Queues Health
Displays the metrics that report on the health of the WebSphere MQ queues.

CA APM Cross-Enterprise: TCPIP Stacks Health
Displays the metrics that report on the health of the TCPIP stacks.

CA APM Cross-Enterprise: DB2 z/OS Performance Overview
Provides an overview of the health of all monitored DB2 subsystems.

CA APM Cross-Enterprise: DB2 z/OS Subsystem Information
Displays environmental information about each monitored DB2 subsystem.

CA APM Cross-Enterprise: DB2 z/OS CPU Activity
Displays the CPU usage information from each monitored DB2 subsystem.

CA APM Cross-Enterprise: DB2 z/OS Buffer Pool Activity
Displays the metrics that show how buffer pools are being utilized in each monitored DB2 subsystem.

CA APM Cross-Enterprise: DB2 z/OS EDM Pool Activity
Displays the metrics that show how the EDM pools are performing in each monitored DB2 subsystem.

CA APM Cross-Enterprise: DB2 z/OS Lock Activity
Displays database lock processing metrics from each monitored DB2 subsystem.

CA APM Cross-Enterprise: DB2 z/OS Log Activity
Displays transaction log metrics from each monitored DB2 subsystem.
CA APM Cross-Enterprise: DB2 z/OS Workload
Displays summary workload performance metrics from each monitored DB2 subsystem (including SQL processing metrics).

CA APM Cross-Enterprise: DB2 z/OS More Information
Displays summary metrics such as work file shortages, RID and Starjoin pool failures, and data set allocation percentages from each monitored DB2 subsystem.

CA APM Cross-Enterprise: DB2 z/OS Data Sharing Groups
Displays summary metrics from each monitored DB2 Data Sharing Group.

CA NetMaster NM for TCP/IP integration provides more dashboards. The names of these dashboards begin with NetMaster (for example, NetMaster - Mainframe Network Overview).

CA NetMaster NM for TCP/IP integration provides additional dashboards. The names of these dashboards begin with NetMaster (for example, NetMaster - Mainframe Network Overview).

View Dashboards in the Introscope Console
You view dashboards in the CA Introscope Console. Select a dashboard from the Dashboard drop-down list or by clicking tabs.

Follow these steps:
1. Connect to the CA Introscope Workstation.
2. Go to Workstation > New Console.
3. Select a dashboard from the Dashboard drop-down list.

After you have selected a CA APM Cross-Enterprise dashboard, use the dashboard drop-down list or click tabs to view other CA APM Cross-Enterprise dashboards.

Alert Indicators
Alert indicators show the current status of an alert by lighting one of three colored symbols that correspond to conditions defined in the alert.
CA APM Cross-Enterprise - Mainframe Health Overview Dashboard

- Red octagon = danger threshold was crossed
- Yellow diamond = caution threshold was crossed
- Green disc = status normal

If the alert has no data, the alert indicator is a gray disc.

An alert indicator with three color states can also be shown as a single symbol.

For more information about alert indicators, see CA APM Workstation User Guide. You can access this guide from CA Technical Support site.

CA APM Cross-Enterprise - Mainframe Health Overview Dashboard

This dashboard offers a quick view of the health of the entire z/OS environment monitored by CA Introscope. It shows alert indicators that report the status for the dashboards available from the Overview dashboard. Double-click the alert indicator to open the corresponding dashboards.

The following table identifies the dashboard alert indicators and corresponding dashboards monitored on this dashboard:

<table>
<thead>
<tr>
<th>Dashboard alert indicator</th>
<th>Dashboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS System Health - LPAR Status</td>
<td>CA APM Cross-Enterprise: z/OS System Health as it relates to LPAR Status</td>
</tr>
<tr>
<td>z/OS System Health - WLM Service Goals</td>
<td>CA APM Cross-Enterprise: z/OS System Health as it relates to Workload Management Service Goals</td>
</tr>
<tr>
<td>CICS Regions Health</td>
<td>CA APM Cross-Enterprise: CICS Regions Health</td>
</tr>
<tr>
<td>Websphere MQ Health</td>
<td>CA APM Cross-Enterprise: Websphere MQ Queue Managers Health</td>
</tr>
<tr>
<td>IMS Subsystems Health</td>
<td>CA APM Cross-Enterprise: IMS Subsystems Health</td>
</tr>
<tr>
<td>DATACOM Address Spaces Health</td>
<td>CA APM Cross-Enterprise: DATACOM Address Spaces Health</td>
</tr>
<tr>
<td>TCPIP Stacks Health</td>
<td>CA APM Cross-Enterprise: TCPIP Stacks Health</td>
</tr>
</tbody>
</table>
Follow these steps:

- To view the dashboard, from the Introscope console, select CA APM Cross-Enterprise Mainframe Health Overview from the Dashboard drop-down menu.

  The Mainframe Health Overview dashboard appears.

- Double-click any of the status indicators to view its corresponding dashboard.
z/OS System Health Dashboard

This dashboard displays the following key metrics to help identify problems with the health of the z/OS system:

- LPAR Status alert indicator
- LPAR Status
- Alerts Unacknowledged Problem and Warning Counts graph
  
  **Note:** The graph only shows the unacknowledged problem and warning counts, not the total unacknowledged count.

- Workload Manager Service Goals
- Degradation Delay Analysis
- Common Storage Area (CSA %)
- Extended Storage Area (ECSA %)
- z/OS CP Busy (%) 
- z/OS LPAR CP Busy (%) 
- Tasks Ready To Dispatch 
- I/O Rate Per Second

For more information, see [CA Cross-Enterprise APM Metrics](#) (see page 143).

To view the dashboard, from the CA Introscope® console, select CA APM Cross-Enterprise: z/OS System Health from the Dashboard drop-down list, or the z/OS System tab.
The two-page z/OS System Health dashboard opens. Scrolling maybe necessary to reach the second page.
CICS Regions Health Dashboard

This dashboard displays the following key metrics to help identify problems with the health of CICS regions:

- CICS Regions Status alert indicator
  Displays the regions status value for all metrics.

- CICS Regions Monitoring alert indicator
  Displays the region monitoring value metrics for all regions.

- CICS Region Statuses
  Displays the regions status value for the top ten CICS regions.

- CICS Alerts Unacknowledged Problem and Warning Counts graph
  Note: The graph only shows the unacknowledged problem and warning counts, not the total unacknowledged count.

- Average CPU Time Per Transaction (µs)
- Average Lifetime Per Transaction (µs)
- Average Suspend Time Per Transaction (µs)
- Transactions Per Second

For more information, see CA Cross-Enterprise APM Metrics (see page 143).
Follow these steps:

- To view the dashboard, from the CA Introscope console, select CA APM Cross-Enterprise: CICS Regions Health from the Dashboard drop-down menu, or the CICS Regions tab.

The CICS Regions Health dashboard opens.

This dashboard displays the following key metrics to help identify problems with CICS transaction groups:

- Average CPU Time Used (µs)
- Average Lifetime (µs)
- Average Suspend Time (µs)
- Transaction Rate (Last System Interval)

For more information, see CA Cross-Enterprise APM Metrics (see page 143).
To view the dashboard, from the CA Introscope® console, select CA APM Cross-Enterprise: CICS Transaction Groups from the Dashboard drop-down list, or the CICS Transaction Groups tab.

The CICS Transaction Groups Details dashboard opens:
IMS Subsystems Health Dashboard

This dashboard displays the following key metrics to help identify problems with the health of IMS subsystems:

- IMS Subsystems Status alert indicator
- Transactions Rate Per Second
- Average Lifetime Per Transaction(µs)
- Transaction Queue Depth
- Average Input Queue Time Per Transaction(µs)
- Average CPU Time Per Transaction(µs)
- Average Processing Time Per Transaction(µs)
- Average Output Queue Time Per Transaction(µs)

For more information, see CA Cross-Enterprise APM Metrics (see page 143).

Follow these steps:

- To view the dashboard, from the CA Introscope console, select CA APM Cross-Enterprise: IMS Subsystems Health from the Dashboard drop-down menu, or the IMS Subsystems tab.
The IMS Subsystems Health dashboard opens.
IMS Transaction Groups Health Dashboard

The Transaction Groups dashboard shows the top ten for the following metrics in the transaction groups:

- Transaction Rate Per Second
- Average Input Queue Time Per Transaction (µs)
- Average Processing Time Per Transaction (µs)
- Average Output Queue Time Per Transaction (µs)
- Average Lifetime per Transaction (µs)
- Average CPU Time Per Transaction (µs)

For more information, see CA Cross-Enterprise APM Metrics (see page 143).

Follow these steps:

- To view the dashboard, from the CA Introscope console, select CA APM Cross-Enterprise: IMS Subsystems Health from the Dashboard drop-down menu, or the IMS Subsystems tab.

The IMS Transaction Group dashboard opens.
CA Datacom Address Spaces Health Dashboard

This dashboard displays the following key metrics to help identify problems with the health of CA Datacom address spaces:

- CA Datacom Address Spaces Status alert indicator
- CA Datacom Address Space Statuses
- CPU Time Per Interval (µs)
- Executed I/O Operations Count Per Interval

For more information, see CA Cross-Enterprise APM Metrics (see page 143).

Follow these steps:

- To view the dashboard, from the CA Introscope console, select CA APM Cross-Enterprise: DATACOM Address Spaces from the Dashboard drop-down menu, or the DATACOM Address Spaces tab.

The DATACOM Address Spaces dashboard opens.
Queue Managers Health Dashboard

This dashboard displays the following key metrics to help identify problems with the health of Websphere MQ queue managers:

- Websphere MQ Queue Managers Status alert indicator
- Websphere MQ Queues Full Status alert indicator
- MQ Alerts Unacknowledged Problem and Warning Counts graph
  
  Note: The graph only shows the unacknowledged problem and warning counts, not the total unacknowledged count.
- CPU Time Per Interval (µs)
- Websphere MQ Queue Manager Statuses
- Executed I/O Operations Count Per Interval

For more information, see CA Cross-Enterprise APM Metrics (see page 143).
Follow these steps:

- To view the dashboard, from the CA Introscope console, select CA APM Cross-Enterprise: WebSphere MQ Queue Managers Health from the Dashboard drop-down menu, or the Queue Managers tab.

The WebSphere MQ Queue Managers Health dashboard opens.
Websphere MQ Queues Health Dashboard

This dashboard displays the following key metrics to help identify problems with the health of WebSphere MQ queues:

- Queues Full Status
- Current Queue Depth %
- Open Input Count
- Open Output Count
- Queue Time (short-term average)
- Queue Time (long-term average)

For more information, see CA Cross-Enterprise APM Metrics (see page 143).

Follow these steps:

- To view the dashboard, from the CA Introscope console, select CA APM Cross-Enterprise: Websphere MQ Queues Health from the Dashboard drop-down list, or the Queues tab.

The Websphere MQ Queues Health dashboard opens.
TCPIP Stacks Health Dashboard

This dashboard displays the following key metrics to help identify problems with the health of TCPIP stacks:

- TCPIP Stacks Status alert indicator
- TCPIP Stack Statuses
- CPU Time Per Interval (µs)
- Executed I/O Operations Count Per Interval

For more information, see CA Cross-Enterprise APM Metrics (see page 143).

Follow these steps:

- To view the dashboard, from the CA Introscope console, select CA APM Cross-Enterprise: TCPIP Stacks Health from the Dashboard drop-down menu, or the TCPIP Stacks tab.

The TCPIP Stacks Health dashboard opens.
DB2 z/OS Performance Overview Dashboard

This dashboard offers a quick view of the health of all DB2 for z/OS subsystems that CA Introscope® monitors. The dashboard shows alert indicators that report the status for the dashboards available from this Overview dashboard. To open the corresponding dashboards, double-click the alert indicator.

The following table identifies the dashboard alert indicators and corresponding dashboards that are monitored on this dashboard:

<table>
<thead>
<tr>
<th>Dashboard alert indicator</th>
<th>Dashboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2 Subsystems</td>
<td>CA APM Cross-Enterprise: DB2 z/OS Subsystem Information</td>
</tr>
<tr>
<td>CPU Activity</td>
<td>CA APM Cross-Enterprise: DB2 z/OS CPU Activity</td>
</tr>
<tr>
<td>Buffer Pool Activity</td>
<td>CA APM Cross-Enterprise: DB2 z/OS Buffer Pool Activity</td>
</tr>
<tr>
<td>EDM Pool Activity</td>
<td>CA APM Cross-Enterprise: DB2 z/OS EDM Pool Activity</td>
</tr>
<tr>
<td>Lock Activity</td>
<td>CA APM Cross-Enterprise: DB2 z/OS Lock Activity</td>
</tr>
<tr>
<td>Log Activity</td>
<td>CA APM Cross-Enterprise: DB2 z/OS Log Activity</td>
</tr>
<tr>
<td>Workload</td>
<td>CA APM Cross-Enterprise: DB2 z/OS Workload</td>
</tr>
<tr>
<td>More Information</td>
<td>CA APM Cross-Enterprise: DB2 z/OS More Information</td>
</tr>
<tr>
<td>Data Sharing Group</td>
<td>CA APM Cross-Enterprise: DB2 z/OS Data Sharing Groups</td>
</tr>
</tbody>
</table>
To view the dashboards, from the CA Introscope® console, select CA APM Cross-Enterprise: DB2 z/OS Performance Overview from the Dashboard drop-down list.

The DB2 z/OS Performance Overview dashboard opens:

- Double-click any of the status indicators opens its corresponding dashboard.
- To navigate to the Mainframe Health Overview dashboard, double-click the Mainframe Health Overview in the upper right-hand corner.
DB2 z/OS Subsystem Information Dashboard

This dashboard displays the following information for each monitored DB2 for z/OS subsystem:

- Subsystem availability
- Total warning exceptions
- Total critical exceptions

For more information, see CA Cross-Enterprise APM Metrics (see page 143).

To view the dashboard, from the CA Introscope® console, select CA APM Cross-Enterprise: DB2 z/OS Subsystem Information from the Dashboard drop-down list.

The DB2 z/OS Subsystem Information dashboard opens:
DB2 z/OS CPU Activity Dashboard

This dashboard displays the following information for each monitored DB2 for z/OS subsystem:

- Total DB2 CPU Percentage
- MSTR CPU Percentage
- DBM1 CPU Percentage
- IRLM CPU Percentage
- MSTR CPU Usage (CP and zIIP)
- DBM1 CPU Usage (CP and zIIP)
- IRLM CPU Usage (CP and zIIP)
- DDF CPU Usage (CP and zIIP)

For more information, see CA Cross-Enterprise APM Metrics (see page 143).
To view the dashboard, from the CA Introscope® console, select CA APM Cross-Enterprise: DB2 z/OS CPU Activity from the Dashboard drop-down list.

The DB2 z/OS CPU Activity dashboard opens:
DB2 z/OS Buffer Pool Activity Dashboard

This dashboard displays the following information for each monitored DB2 for z/OS subsystem:

- Page Read Efficiency
- Prefetch Failures
- Page Write Efficiency
- Page Write Requests
- Synchronous I/O
- Asynchronous Writes
- Available Pages Percentage
- Buffer Pool Size
- Prefetch I/O
- Prefetch Reads
- Page Get Requests
- Prefetch Requests
- Group Buffer Pool Statistics
  - Page Read Efficiency
  - Page Data Reads
  - Page Empty Reads
  - Write Failures

For more information, see CA Cross-Enterprise APM Metrics (see page 143).
To view the dashboard, from the CA Introscope® console, select CA APM Cross-Enterprise: DB2 z/OS Buffer Pool Activity from the Dashboard drop-down list.

The DB2 z/OS Buffer Pool Activity dashboard opens:
### Group Buffer Pool Statistics

#### Page Get Requests

<table>
<thead>
<tr>
<th>Time</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00</td>
<td>2500</td>
</tr>
<tr>
<td>11:10</td>
<td>2300</td>
</tr>
<tr>
<td>11:20</td>
<td>2100</td>
</tr>
<tr>
<td>11:30</td>
<td>1900</td>
</tr>
<tr>
<td>11:40</td>
<td>1700</td>
</tr>
<tr>
<td>11:50</td>
<td>1500</td>
</tr>
</tbody>
</table>

#### Prefetch Requests

<table>
<thead>
<tr>
<th>Time</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00</td>
<td>100</td>
</tr>
<tr>
<td>11:10</td>
<td>120</td>
</tr>
<tr>
<td>11:20</td>
<td>140</td>
</tr>
<tr>
<td>11:30</td>
<td>160</td>
</tr>
<tr>
<td>11:40</td>
<td>180</td>
</tr>
<tr>
<td>11:50</td>
<td>200</td>
</tr>
</tbody>
</table>

#### Page Read Efficiency

<table>
<thead>
<tr>
<th>Time</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00</td>
<td>30</td>
</tr>
<tr>
<td>11:10</td>
<td>25</td>
</tr>
<tr>
<td>11:20</td>
<td>20</td>
</tr>
<tr>
<td>11:30</td>
<td>15</td>
</tr>
<tr>
<td>11:40</td>
<td>10</td>
</tr>
<tr>
<td>11:50</td>
<td>5</td>
</tr>
</tbody>
</table>

#### Page Data Reads

<table>
<thead>
<tr>
<th>Time</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00</td>
<td>100</td>
</tr>
<tr>
<td>11:10</td>
<td>120</td>
</tr>
<tr>
<td>11:20</td>
<td>140</td>
</tr>
<tr>
<td>11:30</td>
<td>160</td>
</tr>
<tr>
<td>11:40</td>
<td>180</td>
</tr>
<tr>
<td>11:50</td>
<td>200</td>
</tr>
</tbody>
</table>

#### Page Empty Reads

<table>
<thead>
<tr>
<th>Time</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00</td>
<td>30</td>
</tr>
<tr>
<td>11:10</td>
<td>25</td>
</tr>
<tr>
<td>11:20</td>
<td>20</td>
</tr>
<tr>
<td>11:30</td>
<td>15</td>
</tr>
<tr>
<td>11:40</td>
<td>10</td>
</tr>
<tr>
<td>11:50</td>
<td>5</td>
</tr>
</tbody>
</table>

#### Write Failures

<table>
<thead>
<tr>
<th>Time</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00</td>
<td>0</td>
</tr>
<tr>
<td>11:10</td>
<td>0</td>
</tr>
<tr>
<td>11:20</td>
<td>0</td>
</tr>
<tr>
<td>11:30</td>
<td>0</td>
</tr>
<tr>
<td>11:40</td>
<td>0</td>
</tr>
<tr>
<td>11:50</td>
<td>0</td>
</tr>
</tbody>
</table>

DB2 z/OS EDM Pool Activity Dashboard

This dashboard displays the following information for each monitored DB2 for z/OS subsystem:

- EDM Pool Full Failures
- DBD Pool Full Failures
- Statement Pool Full Failures
- Cursor Table Load Percentage
- Package Table Load Percentage
- DBD Load Percentage
- Dynamic Statement Load Percentage
- DBD Pool Free Pages
- Statement Pool Free Pages
- DBD Pool Available Percentage
- Skeleton Package Table Available Percentage
- Skeleton Cursor Table Pages
- Skeleton Package Table Pages

For more information, see CA Cross-Enterprise APM Metrics (see page 143).
To view the dashboard, from the CA Introscope® console, select CA APM Cross-Enterprise: DB2 z/OS EDM Pool Activity from the Dashboard drop-down list.

The DB2 z/OS EDM Pool Activity dashboard opens:
DB2 z/OS Lock Activity Dashboard

This dashboard displays the following information for each monitored DB2 for z/OS subsystem:

- Deadlocks
- Timeouts
- Local Suspensions
- Global Suspensions
- Local Requests
- Global Requests
- Escalations

For more information, see CA Cross-Enterprise APM Metrics (see page 143).
To view the dashboard, from the CA Introscope® console, select CA APM Cross-Enterprise: DB2 z/OS Lock Activity from the Dashboard drop-down list.

The DB2 z/OS Lock Activity dashboard opens:
DB2 z/OS Log Activity Dashboard

This dashboard displays the following information for each monitored DB2 for z/OS subsystem:

- Active Log Space Available Percentage
- Checkpoints
- Minutes Between Checkpoints
- Active Reads
- Archive Reads
- Unavailable Buffer Waits
- Write Forced
- Write Waits
- Write No Waits

For more information, see [CA Cross-Enterprise APM Metrics](#) (see page 143).
To view the dashboard, from the CA Introscope® console, select CA APM Cross-Enterprise: DB2 z/OS Log Activity from the Dashboard drop-down list.

The DB2 z/OS Log Activity dashboard opens:
DB2 z/OS Workload Dashboard

This dashboard displays the following information for each monitored DB2 for z/OS subsystem:

- Maximum Users Percentage
- Maximum TSO Users Percentage
- Maximum Batch Users Percentage
- Maximum Remote Users Percentage
- Current Threads
- Maximum Threads
- Queued Create Thread Requests
- Create Thread Requests
- Single Phase Commits
- Aborts
- Select / Open Requests
- Insert / Update / Delete Requests
- Distributed SQL Activity
  - SQL Statements Sent
  - SQL Statements Received
  - Rows Sent
  - Rows Received

For more information, see CA Cross-Enterprise APM Metrics (see page 143).
To view the dashboard, from the CA Introscope® console, select CA APM Cross-Enterprise: DB2 z/OS Workload Activity from the Dashboard drop-down list.

The DB2 z/OS Workload Activity dashboard opens:
This dashboard displays the following information for each monitored DB2 for z/OS subsystem:

- Dataset Open Percentage
- 4K Workfile Shortages
- 32K Workfile Shortages
- RID Pool Failures
- Starjoin Pool Failures
- Current Starjoin Pool Used Percentage
- Maximum Starjoin Pool Used Percentage
- Current Starjoin Pool Size
- Maximum Starjoin Pool Size

For more information, see CA Cross-Enterprise APM Metrics (see page 143).
To view the dashboard, from the CA Introscope® console, select CA APM Cross-Enterprise: DB2 z/OS More Information from the Dashboard drop-down list.

The DB2 z/OS More Information dashboard opens:
Chapter 4: How to Trace and Analyze Events

CA Introscope allows the system administrator to select trace filter criteria and then analyze the results to improve system performance.

This section contains the following topics:

About CA Introscope (see page 97)
About Cross-Process Transaction Traces (see page 98)
Generating Cross-Process Transaction Traces (see page 100)
Narrow Trace by Excluding Front-End Elements (see page 109)
Analyze Trace Results (see page 110)
CTG Transaction Trace Components Properties (see page 121)
HTTP Transaction Trace Components Properties (see page 127)
Review or Adjust Results Components (see page 132)

About CA Introscope

The following list contains CA Introscope features for tracing events:

■ Create, view, browse, and search trace transactions events.
■ Trace the transaction activity at the event level.
■ Reduce the time that is required to identify a problem event.
■ Cross-process transaction traces.
■ Trace synchronous transactions that cross boundaries in the homogeneous application server environments.

See the CA APM Cross-Enterprise Integration Guide and CA APM Cross-Enterprise Workstation User Guide for a complete picture of the CA Introscope features functionality.

Note: Optional conditional error matching filter criteria are detailed in the CA APM Cross-Enterprise Workstation User Guide and are not covered in this guide.

Important! You need the appropriate Workstation permission to create a transaction trace. Contact your CA Introscope administrator for the appropriate permissions.
About Cross-Process Transaction Traces

Modern applications are often multi-tier with processes running in the differing tiers calling each other. Often performance problems happening in the front-end application process are due to problems happening on the back-end process it uses. Tracing the front-end process is not sufficient to determine the cause of the issue. And it is often impossible to tell which back-end processes it is calling.

Cross-process transaction tracing solves this problem by correlating the trace events of the front-end applications with the corresponding trace events from back-end processes. Use the CA Introscope Workstation to diagnose back-end processes problems by viewing a problematic front-end transaction trace event. Then use the trace event to find the corresponding back-end trace events.

That back-end trace provides the “when, where, and why” of information that determines the cause of the problem. The Information provided includes server name, transaction processor, unit of work ID, transaction ID, and internal transaction timings.

Cross-Process tracing is enabled when the appropriate front-end and back-end Agents and tracers are installed. For more information about installing the tracers, see Install and Configure the Extension (see page 11).

Back end

Back ends are external systems, such as a:

- Database
- Mail server
- Transaction processing system such as CICS or IMS
- Messaging system such as WebSphere MQ

Front end

Front ends are the component of an application that first handles an incoming request such as a:

- Servlet
- JSP
- Management database
- EJB
When a front-end transaction invokes a back-end transaction, two trace events are created and sent to the CA Introscope EM. One from the front-end agent and the other from the back-end CA APM Cross-Enterprise Agent. Additional back-end traces are generated for each additional back-end call that the front-end application makes. The CA Introscope Workstation can display all these traces together on the Trace View tab. Selecting the front-end trace event allows the CA Introscope Workstation to fetch and display all correlated back-end traces on the same pane. Also, selecting a back-end trace event causes the front-end and all correlated back-end traces to display together.

The front-end tracers for CTG and web services insert a unique correlation identifier in the front-end traces. The CA APM Cross-Enterprise Agent decorates the back-end calls into CICS with the same correlation identifier. This decoration flags the back-end transaction call as originating from a monitored front-end transaction and provides a unique identifier. CA APM Cross-Enterprise adds the same correlation identifier to the corresponding CICS back-end trace. The CA Introscope Workstation uses the unique identifier in the front-end and back-end trace events to fetch corresponding front-end or back-end traces for display. Only the CICS transactions can be invoked using CTG, and web services.

The front-end tracer for the MQ flags and MQ messages come from a monitored application. The MQ trace is correlated with MQ message ID, correlation ID, or both. The MQ message ID or correlation ID provides a unique identifier for the correlation between both the front-end MQ traces and back-end traces. The back-end traces from both CICS and IMS transactions have this correlation ID when MQ is the communication method that is used to invoke the transaction.
Generating Cross-Process Transaction Traces

As a system administrator, your responsibilities often include monitoring systems, addressing known issues, and then triaging these issues. You trace these systems issues using CA Introscope to find the components that caused them. To find these components, you construct filter criteria on the Transaction Trace screen. You then analyze the results to determine the problem.

The following illustration provides an overview of the basic trace processes:

This process has the following tasks:
1. [Enable Cross Process Transaction Tracing](#) (see page 101).
2. [Select Event Duration and Type filters](#) (see page 102).
3. [Select CICS/IMS filters](#) (see page 104).
4. [Select Trace Duration, agent filters, and start trace](#) (see page 108).
5. [Narrow Trace by Excluding Front-End Elements](#) (see page 109).
6. [Analyze Trace Results](#) (see page 110)
7. [Review or Adjust Results Components](#) (see page 132)

**Important!** Running a transaction trace can have a negative impact on the performance of the monitored application.

Completing this process lets you understand which filters criteria to select to find the problematic components and how to analyze the results.
Enable Cross Process Transaction Tracing

The CA APM Cross-Enterprise component is designed to allow transaction tracing across the multiple tiers of an application that invokes transactions on the mainframe. The currently supported communications methods available out of the box are:

- CICS Transaction Gateway using Channels invoking the CICS transactions
- HTTP invocations from Java applications that extend HttpURLConnection which invoke CICS transactions
- HTTP invocations from Java applications that extend HttpURLConnection which invoke Java servlet applications extending HttpServlet
- Web Services Calls into CICS
- WebSphere MQ Series messages sent to CICS or IMS transactions which the mainframe transaction retrieves using function MQget()

When properly configured traces can be generated from all instrumented tiers of an application and shown in the Workstation together in the Trace View tab. The Trace View tab is accessible in the Workstation Investigator from the Transaction Trace Viewer launched during a Transaction Trace session. The Trace View tab is also accessible from the Agents tab of the Cross-Enterprise APM agent in the Investigator.

The Workstation is able to correlate the separate traces that run together into one view because the traces generated for the corresponding transactions contain the same correlation ID. This correlation ID is generated in the first tier of the application and passed to the agents instrumenting transactions invoked on subsequent tiers via the communications methods that are supported. In order for this to work each tier must be instrumented and every communications method that is used must be supported and instrumented.

Additional Information on how to instrument the application tiers for the various communications methods is located in Install and Enable Java Agent Components.
Select Event Duration and Type Filters

In the CA Introscope Workstation select the event duration and type transaction filters to construct your trace filter criteria.

Event duration

Allows you to select the minimum amount of time an event runs before it is added to the trace results.

**Filtered Property:** The Event duration filter does not use a property but is instead applied against the duration of the transaction.

**Value:** Contains the minimum duration of the transaction in milliseconds

**Supported Trace Sources:** Web Services, CTG, or MQ front-end; CICS or IMS back-end traces

**Note:** The minimum granularity for the duration filter is one millisecond which can be longer than the typical back-end z/OS transaction runs. To get the microsecond duration filter granularity on back-end transactions, omit this filter and use the Microsecond Lifetime filter instead. If you use the Microsecond Lifetime filter, the Workstation does not receive any transaction traces from the front end distributed tiers of the application. Run multiple transaction traces in parallel to get the traces you want from the different tiers.

**Important!** A duration filter that is applied to a front-end agent causes all transaction correlated to any front-end transaction to be returned from the CA APM Cross-Enterprise Agent or any other back-end agent. This can have a substantial negative impact on the performance. Applying this filter to a subset of available front-end agents mitigates the performance degradation.

Type Transaction Filters

Allows you to select the transaction filters types including user ID, URL, URL Query, header, parameters, and session attributes.

**Note:** If you want to correlate traces across the tiers, then match at least one trace session to transactions running on your front-end tier. Ensure all the filters that are used are crafted to include the transactions you are interested in generating traces from on the front-end tier of your application. If the agent decides to generate a trace on the front-end tier, it communicates with the back-end agents. This informs them to propagate this decision and generate correlated traces on the other tiers. There is a propagation flag that passed using the instrumented communication method that informs downstream agents of this decision.

Follow these steps:

1. Log in to the CA Introscope Workstation.
2. Select Workstation and then New Transaction Trace Session.
3. Select the Minimum transaction duration check box.
4. Enter the Minimum transaction duration value and from the drop-down list select Milliseconds or seconds.
   Specify the minimum time that a transaction is traced.
   **Format:** Numeric milliseconds or seconds.
   **Default:** 5 seconds

5. (Optional) Enter transaction filters.
   **Note:** Data is only available for use in these filters if the CA Introscope Agent is configured to capture it.
   Click the check box and select one of the following:

   **User ID**
   Select user ID from the drop-down list and enter the user ID value.
   **Filtered Property:** user ID
   **Value:** Matches the user ID property of the transaction trace. Indicates the user ID which ran the transaction.
   **Supported Trace Sources:** IMS back-end only
   **Note:** Some values of this filter such as user ID does not exist. These values can unexpectedly cause all unsupported source traces to appear in the trace results because they do not contain the user ID property.

   **URL**
   Select URL from the drop-down list and enter the URL.
   **Value:** The portion of the URL that is passed through to the servlet or JSP.
   **Supported Trace Sources:** Not applicable to any trace source. Entering a value for this filter results in no trace results.
   **Format:** Remove the leading protocol specifier, computer name, and port number.
   **Example:** /ExampleAppClientV6Web

   **URL Query**
   Select URL Query from the drop-down list and enter the URL.
   **Value:** The portion of the URL that specifies query parameters in the HTTP request.
   **Supported Trace Sources:** Not applicable to any trace source. Entering a value for this filter results in no trace results.
   **Format:** Remove the leading protocol specifier, computer name, and port number.
   **Example:** /ExampleAppClientV6Web
Generating Cross-Process Transaction Traces

**Request Header**

Enter Request Header from the drop-down list and enter the request header value.

**Value:** The HTTP request header.

**Supported Trace Sources:** Not applicable to any trace source. Entering a value for this filter results in no trace results.

**Request Parameter**

Enter Request Parameter from the drop-down list and enter the request parameter value.

**Supported Trace Sources:** Not applicable to any trace source. Entering a value for this filter results in no trace results.

**Session Attribute**

Enter a session attribute from the drop-down list and enter the session attribute.

**Value:** Your session information that consists of a name and value.

**Supported Trace Sources:** Not applicable to any trace source. Entering a value for this filter results in no trace results.

6. **(Optional)** Enter conditional error-matching-processing Boolean filters.

**Important!** These transaction filters can negatively affect the performance.

The event duration and type filters are set. Proceed to selecting the CICS or IMS filters.

**Select CICS or IMS Filters**

After entering the event duration and type filters on the Transaction Trace screen, continue by entering the CICS or IMS filter criteria. You can skip this step if you do not want to restrict the trace generation to the mainframe system. If you want to generate traces from the front end distributed tiers, it is best to skip this step.

**Note:** The CICS and IMS filters are mutually exclusive.

Select the check box, and enter the value for each filter as needed.

**CICS server name (CTG) equals**

**Filtered Property:** Job Name or Server Name

**Supported Trace Sources:** CICS back-end traces that were invoked using CTG.

**Value:** The name of the server that was used to invoke the CTG call.
CICS/IMS communication method equals

Filtered Property: Communication Method

Supported Trace Sources: CICS or IMS back end

Value: Cross-process tracing into CICS or IMS is available for the front-end application that invoke the transaction through the following communication CICS or IMS methods.

Enter one of these methods:

CICS methods

- Web Service
  
  The web services CA SYSVIEW tracer is installed on top of the Service-Oriented Architecture (SOA) tracer. A correlation ID with the front-end transaction trace is included so it can be matched up with the corresponding back-end trace from the mainframe.

  Recommend filter criteria:
  
  Select the minimum transaction duration, enter a numeric value, and then select a duration unit from the drop-down list.

  Example: 5000 milliseconds

  (Optional) Select URL of the application from the drop-down list and enter the URL.

  Note: Remove the leading protocol specifier, computer name, and port number.

  Example URL: /ExampleAppClientV6Web

- CTG Channel
  
  The CTG CA SYSVIEW tracer includes a correlation ID with the front-end transaction trace that can be associated with the corresponding mainframe back-end trace.

  Recommend filter criteria:
  
  Select the minimum transaction duration, enter a numeric value, and then select a duration unit from the drop-down list.

  (Optional) For CTG front-end traces with the Program Name and Transaction Name properties, select CICS Program Name (CTG) equals, and enter the program name or transaction name.

  Note: CTG front-end traces never have server name, web service name, or microsecond lifetime properties. If these properties are entered in the filter criteria, no front-end traces appear in the Trace Viewer.
Generating Cross-Process Transaction Traces

- MQ Trigger Message
  The traces into the MQ Series do not use correlation IDs, so the front-end and back-end correlation cannot be made using this correlation ID. Instead, the correlation is done using a preexisting MQ message ID and MQ correlation ID.

  **Recommend filter criteria:**
  Select the minimum transaction duration, enter a numeric value, and then select a duration unit from the drop-down list.
  This filter restricts the display to those transactions that run longer than the specified time.
  **Example:** 5000 milliseconds
  **Note:** The IBM Websphere MQ Connectors and Messaging System Extension tracer is used as the MQ series front-end tracer.

- HTTP
  The HTTP CA SYSVIEW tracer includes a correlation ID with the front-end transaction trace that can be associated with the corresponding mainframe back-end trace.

  **Recommend filter criteria:**
  Select the minimum transaction duration, enter a numeric value, and then select a duration unit from the drop-down list.
  **Example:** 5000 milliseconds
  (Optional) Select CICS/IMS Communication Method equals HTTP.
  (Optional) Select URL of the application from the drop-down list and enter the URL. Be careful when using the URL because it is specific to the tier being traced. If used, set the URL of the servlet of first tier of the application that has an installed HTTP tracer.
  **Note:** Remove the leading protocol specifier, computer name, and port number from any URL.
  **Example Servlet URL:** /HTTPTest/servlet/FrontEndClient
  **Example CICS URL:** /CICS/CWBA/DFJ$JWB1

**IMS methods**

- MQ IMS Bridge
  The front-end application used the IMS Bridge Queue to invoke the IMS transaction.

- MQ IMS Adapter
  The MQ IMS Adapter was used to get the MQ message that was sent from the front-end application.
Generating Cross-Process Transaction Traces

Chapter 4: How to Trace and Analyze Events

CICS program name (CTG) equals
- **Filtered Property:** Program Name
- **Supported Trace Sources:** CTG front end; CICS back end
- **Value:** The name of the program that was executed on the CICS region.

IMS transaction ID equals
- **Filtered Property:** Transaction ID
- **Supported Trace Sources:** IMS back-end
- **Value:** The transaction name.

IMS job name equals
- **Filtered Property:** Job Name (Dependent Region)
- **Supported Trace Sources:** IMS back-end
- **Value:** IMS-dependent region job name that processed the transaction.

CICS web service name equals
- **Filtered Property:** Web Service Name
- **Supported Trace Sources:** Web Services front end; CICS back end
- **Value:** Name of the web service that is used to execute this transaction. This property is applicable only to web service transaction tracers.

CICS/IMS transaction lifetime lasting longer than
- **Filtered Property:** Microsecond Lifetime
- **Supported Trace Sources:** CICS or IMS back end
- **Value:** The transaction lifetime in microseconds
- **Minimum value:** One microsecond

CICS/IMS transaction processor name equals
- **Filtered Property:** Transaction Processor
- **Supported Trace Sources:** CICS or IMS back end
- **Value:** The transaction processor that ran the transaction, CICS or IMS

IMS PSB name equals
- **Filtered Property:** PSB Name
- **Supported Trace Sources:** IMS back end
- **Value:** The PSB name that is associated with the transaction.
**Generating Cross-Process Transaction Traces**

**CICS transaction name (CTG) equals**

- **Filtered Property**: Transaction Name
- **Supported Trace Sources**: CTG front end; CICS back end
- **Value**: Name of the transaction on the CICS region.

The CICS/IMS filters are set. Proceed to setting the trace duration and agents filters.

**Select Trace Duration, Agent Filters, and Start Trace**

After entering the CICS or IMS filters, on the Transaction Trace screen, continue by entering the trace duration and Agent Filters. At the end of this procedure, start the trace.

**Trace Duration**

Allows you to set the maximum mount a time in minutes a trace session can take.

**Agent Filters**

Allows you to select which agent to trace.

You can apply different filters to the front-end application transactions, and the back-end z/OS transactions. In this case one or more transaction traces can be run simultaneously where each selects different agents. For example, use a duration filter on the front end traces, while using the Microsecond Lifetime filter on the back-end traces.

**Follow these steps:**

1. Enter the trace session duration in minutes.
   - **Values**: Numeric
   - **Default**: 10
2. Click either the Trace all supported Agents or Trace Selected Agents check box.
   - **Trace all supported Agents**
     - Traces supported agents that are currently connected, and any that connect during the Trace session.
     - **Default**
   - **Trace selected Agents**
     - Select agents from the list. Use CTRL + click to select multiple agents.
3. Click OK to start the Transaction Trace session.
   - The Transaction Trace Viewer opens.
You have now set the filter criteria for:
- Event duration
- Type
- CICS or IMS
- Trace Duration
- Agents

**Narrow Trace by Excluding Front-End Elements**

You can exclude front-end elements from the trace by selecting options on the New Transaction Trace session.

**To exclude front-end traces**

Follow these steps:
1. Create a transaction trace session.
2. Click the following check boxes and enter the value for each filter.
   - CICS/IMS transaction lifetime lasting longer than
   - CICS transaction name (CTG) equals
   - CICS server name (CTG) equals
   - CICS program name (CTG) equals
3. Enter any other needed information and click OK.

**To return CTG front-end traces**

Follow these steps:
1. Create a transaction trace session.
2. Click the following check boxes and enter the value for each filter.
   - CICS/IMS transaction name (CTG) equals
   - CICS program name (CTG) equals
3. Enter any other needed information and click OK.
**To exclude CTG front-end traces**

Follow these steps:
1. Create a transaction trace session.
2. Click the following check boxes and enter the value for each filter.
   - CICS/IMS transaction lifetime lasting longer than
   - CICS web service name equals
   - CICS server name (CTG) equals
3. Enter any other needed information and click OK.

**To exclude HTTP front-end traces**

Follow these steps:
1. Create a transaction trace session.
2. Click the following check boxes and enter the value for each filter.
   - CICS/IMS transaction lifetime lasting longer than
   - CICS/IMS Communication Method equals
   - CICS server name (CTG) equals
   - CICS program name (CTG) equals
3. Enter any other needed information and click OK.

**To exclude MQ front-end traces**

Follow these steps:
1. Create a transaction trace session.
2. Click the following check boxes and enter the value for each filter.
   - CICS/IMS transaction lifetime lasting longer than
   - CICS transaction name (CTG) equals
   - CICS server name (CTG) equals
   - CICS web service name equals
   - CICS program name (CTG) equals
3. Enter any other needed information and click OK.

**Analyze Trace Results**

Use the information in this section to understand your trace results.
Change Duration Time Intervals

Set the display units used for duration and call time by right-clicking the Duration column header on the Transaction Trace Viewer window. Select one of the following from the drop-down menu:

- Microseconds
- Milliseconds
- Seconds

Cross-Process Traces Time Alignment

Time alignments between system clocks in a cross-process trace often are not synchronized. Cross-process traces align the trace with the front-end trace that invoked it.

**Note:** Usually traces are displayed in order based on the system clock where they originated. All back-end traces sourced from the same CA APM Cross-Enterprise agent can be synchronized properly relative to each other but not the correlated front-end transaction.

**CTG and web services**

CTG and web services calls are not displayed relative to their actual synchronization with the front end calling transaction. The associated events for these back-end traces are grouped together, enlarged, and aligned to the left in the Trace View.

**MQ calls**

MQ calls are asynchronous and occur after the front-end application terminates. The delay is shown regardless of discrepancies introduced by clock synchronization. In the Trace View these events are not aligned, enlarged, or grouped together.

**IMS transaction trace timestamp**

The IMS transaction trace timestamp starts when the transaction is placed on the input queue.

- When searching for the corresponding IMS SMF record for a transaction trace always use the Unit of Work ID from the trace and the command:
  ```shell
  IMSTLOG UOW <value_of_Unit_of_Work_ID>;
  ```
- Do not attempt to use the timestamp from the IMS transaction trace in the Workstation to find the corresponding IMS SMF record in CA SYSVIEW. The IMS SMF record time shows process start time instead. For transactions that stay on the input queue for a long time these two values can differ significantly.
About Transaction Trace View

You could organize the information in one of two ways here.

The Transaction Trace View consists of top and bottom panes that help you analyze your trace results. The top pane contains all the transaction trace events selected from the filter criteria. The bottom pane contains a set of views that let you view the transaction trace results in different ways.

- **Summary View** (see page 112)
- **Trace View** (see page 113)
- **Tree View** (see page 114)
- **Sequence View** (see page 116)

Summary View

The Summary View shows metrics for the components in the selected transaction. Metrics include the path, number of calls, the length of the call in milliseconds, and the minimum, average, and maximum call times.

The Call Time (ms) column is the duration spent in the component excluding any time spent in any child components.

**Note:** The first time you select a transaction in the transaction table, the Summary View opens. When you select a transaction that has been opened before, it opens in the most recently selected view.

This information appears for the currently selected transaction:

- Fully qualified agent name
- Start time, in the agent computer system clock, of the invocation of the root component
- Execution time of the root component in milliseconds
Trace View

The Trace View shows the selected transaction trace in a graphical stack display. To expand and collapse the stack of components, click the triangular arrow to the left of a transaction. When you select one of the components of a transaction, you can see component details in the bottom pane of the viewer. The details include any properties from the component. Most properties are located in at the top component of the stack, however subcomponents can also contain properties.

In addition to the selected transaction trace, this view shows any correlated cross-process transaction traces. Click any trace to make it the focus and investigate its components further. For more information, see About Cross-Process Transaction Traces (see page 98).

The transaction traces generated from front-end agents where the CTG CA SYSVIEW Tracer is installed have options that allow the launching of a back-end trace session. For more information about launching a back-end trace, see Launch a New Back-End Transaction Trace Session from an Existing One (see page 120).
Tree View

The Tree View is a hierarchical view of the components of the currently selected transaction trace. Each component represents a Java method or mainframe timing that the transaction completed. A component shows its duration and a percent of the total transaction lifetime that that duration represents.

The front-end traces that are generated from an instrumented Java application have the usual components that represent methods in the Java call stack. To drill down to the methods that invoked the back-end applications on the mainframe, expand the call stack in the tree.

**Note:** For the back-end traces generated by the CA APM Cross-Enterprise agent on z/OS, the tree view does not represent an actual Java call stack. Instead, it is a set of nested timings that are taken during processing of a CICS or IMS transaction.

The hierarchical structure of the transaction traces generated when processing a CICS or an IMS transaction are as follows.

The Transaction traces consist of a series of CICS and IMS components.

**CICS Transaction Traces**

Provides information about how time was spent in CICS transactions. Tracing a CICS transaction produces a CICS Suspend trace. If the transaction invokes DB2 queries, you also get a CICS DB2 trace.

The following property in the Cross-Enterprise_APM_Dynamic.properties file controls the generation of the CICS DB2 trace:

SYSVIEW.CICS.Transaction.Trace.DB2

The CICS Suspend trace has the following hierarchy of components as identified by their paths:

- CICS Regions\region|transaction_name|task_number|Suspend|Transaction Lifetime
  - Dispatch Time
  - Program Load Time
  - Suspend Time
  - <Optional suspend time components>

The CICS DB2 trace has the following hierarchy of components as identified by their paths:

- CICS Regions\region|transaction_name|task_number|DB2|Transaction Lifetime
  - Program program_name\SSID ssid\statement type Stmt# statement number

The CICS transaction traces have the following components:

**Transaction Lifetime**
Is the total time or transaction lifetime that equals the sum of input, processing, and output time.

**Note:** For more information, see [CICS Transaction Lifetime Component Properties](#) (see page 132).

**Dispatch Time**

Is a child of Transaction Lifetime and represents time spent dispatched and doing work. The CPU time is the portion of dispatch time when the task is using processor cycles.

**Note:** For more information, see [CICS Dispatch Time Component Properties](#) (see page 135).

**Program Load Time**

Is a child of dispatch time that shows how long the program took to load.

**Suspend Time**

Accompanies Dispatch Time and it represents time that is wasted in waiting for system resources.

Suspend time has extra child components representing nonoverlapping timings.

Suspend Time also includes various overlapping timings that cannot be represented as a hierarchy. These timings are represented as properties in the lower pane of the Trace View tab.

**Note:** High suspend times on a running transaction indicates an issue.

**Note:** Zero duration timing properties and components are *not* presented.

**Note:** For more information, see [CICS Suspend Time Component Properties](#) (see page 135).

**Program program_name |SSID ssid|statement type Stmt# statement number**

Specifies the CICS DB2 statement component which provides the timings for the DB2 queries that the identified program invokes. The statement runs on the subsystem that is identified by ssid. The path contains the standard DB2 statement type such as SELECT, DELETE, FETCH, and INSERT. If CA-SYSVIEW is configured to generate statement numbers, then one is added to the path. The statement number indicates the line of the program which invoked the statement.

**Note:** For more information, see [CICS DB2 Statement Component Properties](#) (see page 137).
**IMS Transaction Trace**

Specifies the information about how time was spent in an IMS transaction. Tracing an IMS transaction produces a single trace.

The IMS trace has the following hierarchy of components identified by their paths:

IMS Subsystems| subsystem name | Transaction| transaction name | Transaction Lifetime
Input Queue Time
Process Time
optional components
Output Queue Time

The IMS transaction trace has the following components:

**Transaction Lifetime**

The total time or transaction lifetime equals the sum of input, processing, and output time which are its child components.

*Note:* For more information, see [IMS Transaction Lifetime Component Properties](#) (see page 138).

**Input Queue Time**

The amount of time the input transaction waited in the message queue before being scheduled.

**Process Time**

Process Time has extra child components representing nonoverlapping timing events. These optional components are IMS Monitor type events such as, IWAITs, DL/I, and External Subsystem calls that occur during the transaction lifetime.

A single optional child component that contains properties for Event Count and Maximum Event Time represent multiple events. The Event Count property indicates the number of events. The Maximum Event Time property has the duration of the slowest instance of the event.

**Output Queue Time**

The amount of time the transaction output waited in the output message queue before being forwarded to its destination.

**Sequence View**

The Sequence View tab displays the caller-callee relationship between the segments of a transaction to make the sequencing order of the calls visually apparent.

Use the Sequence View if the following is true:

- A transaction includes asynchronous calls
- Call processes running on agents that are not time synchronized with each other
- Complex synchronous calls across multiple JVMs or CLRs
CICS with MQ Trigger Message Example Using the Tree View

This example shows the results from the following filter selections.
- Duration time greater the 40 microseconds
- CICS/IMS communication method equals CICS with MQ Trigger Message

The following procedure explains how to analyze these trace results using the tree view.

Follow these steps:
1. Click the Tree View tab in the Transaction Trace Viewer window to see the tree structure of the web service transaction trace components.
2. Highlight the transaction trace component to see the properties associated with that component.
Web Services Example Using Large Duration Time

This example shows how to analyze a duration time using the Trace View. The duration time on the transaction trace screen was set to time greater than 5000 milliseconds.

The Transaction Trace Viewer shows a front-end task with a 5063-millisecond duration.

The Trace View shows that the front-end transaction calls a correlated back-end CICS transaction. The CICS transaction has a 3675-millisecond duration. Over 70 percent of the transaction time was spent waiting on completion of the CICS transaction. Most of that time was spent with the program dispatched.

CTG Example for High Suspend Time

This example shows how to analyze a high suspend time using the Trace and Tree Views.

The filter criteria that was used for this example was an event duration of 78. The results for this selected criteria follow.

Follow these steps:
1. Highlight the transaction with the high duration time.
2. Click the Trace View.
3. The Trace View opens displaying the correlated front end and back-end traces.

4. Select the Tree View tab to diagnose the problem and highlight the transaction trace component to see the properties associated with it.

The following example shows that the CICS transaction spends 77 percent of its time suspended. The dispatch time is longer than the run time. Correct this issue.
Problematic Transaction for Unit of Work

If the transaction is problematic, use the Unit of Work ID to investigate the back-end transaction using CA SYSVIEW. CA SYSVIEW administrators can find the corresponding SMF record for this transaction using the CA SYSVIEW GUI.

The value in this field can be used to look up the associated SMF record in SYSVIEW.

For IMS transactions:

\[\text{IMSTLOG UOW <value_of_Unit_of_Work_ID>;}\]

For CICS transactions:

\[\text{CTRANLOG; SELECT UOWID EQ <value_of_Unit_of_Work_ID>;}\]

Additional transaction trace events that show the transaction activity within the back-end system can also be viewed from the Workstation. These events are produced from the CA APM Cross-Enterprise running on the mainframe, and are correlated with traces generated from the front-end Agent.

The CICS back-end trace events provide information about the performance of transactions that run on CICS. Trace events provide the following information in the Trace Viewer to help you diagnose the problem:

- Transaction name
- Transaction lifetime
- CPU time
- Suspend time
- Dispatch time

The IMS back-end trace events provide information about the performance of transactions that run on IMS. Trace events provide the following information in the Trace Viewer to help you diagnose the problem.

Launch a New Back-End Transaction Trace Session from an Existing One

Correlating front-end and back-end traces can be challenging when the filter is not narrowed to include fewer traces. When there is a heavy volume of traces coming from the front-end and back-end, CA APM Cross-Enterprise lets you launch a new transaction trace session from an existing one. This launch creates a new back-end transaction trace session from the selected web service or CTG front-end transaction trace and makes correlation are more likely.
Follow these steps:

1. Click the problematic web service or CTG front-end transaction trace, on the Transaction Trace Viewer.

2. Highlight the last item on the Trace View tab, right-click, and select Launch New Trace from the pop-up menu.

   A New Transaction Trace Session window opens with populated fields from the front-end trace.

3. Click OK to view transactions that meet the specified criteria in the Transaction Trace Viewer window:

   The returned trace is the correlated front-end and back-end trace.

CTG Transaction Trace Components Properties

The section describes the components and properties added to Java traces by the CTG CA SYSVIEW Tracer. Each of the transaction trace components and its properties are described.
CTG Tracing Properties

The use of the class method `com.ibm.ctg.client.JavaGateway.flow()` by an instrumented application generates the CTG flow method trace component with the following properties. Properties that can be filtered in the Transaction Trace Session dialog list the filter name.

Requests of the type `com.ibm.ctg.client.CicsCpRequest` have the following properties:

**Class**

The instrumented class is `com.ibm.ctg.client.JavaGateway`.

**CTG Request Class**

*class name*

**Default:** `com.ibm.ctg.client.CicsCpRequest`

**CTG Request Type**

*Code Page*

**Method**

The method name is always equal to `flow`.

Requests of the type `com.ibm.ctg.client.ECIRequest` have the following properties:

**Communication Method**

*communication method*

- CTG Channel
- CommArea Static
- CommArea Dynamic

**Filter:** CICS/IMS communication method equals

**Correlation UUID**

*correlation UUID:* `IScopeCTGID`

Properties with this value have a name that specifies a UUID used for correlation. The value is applicable only to CTG transaction traces. A different UUID is used for each CTG transaction, with multiple calls to a single extended transaction using one UUID.

**Format:** The name is a 32-byte UUID, and the value is `IScopeCTGID`.

**Class**

The instrumented class is `com.ibm.ctg.client.JavaGateway`
CTG Extend Mode

extend mode

Specifies the value that is used in the method call for the ECIRequest.Extend_Mode. Possible values are:

- **ECI_BACKOUT**—The transaction is being backed out.
- **ECI_COMMIT**—The transaction is being committed.
- **ECI_EXTENDED**—This is one program call in an extended transaction.
- **ECI_NO_EXTEND**—This is the first program call in a non-extended transaction or the last in an extended transaction that is committing.

CTG Server Name:

server

The host name of the connected CTG Server.

Default: server

CTG Request Class

class name

Default: com.ibm.ctg.client.ECIRequest

Method

The instrumented method name is always equal to 'flow'.

Program Name

program name

The name of the transaction that is invoked on the CTG Server. This property does not exist for backout and commit calls.

Filter: CICS program name (CTG) equals.

Transaction Name

The name of the transaction that is invoked on the CTG Server.

Filter: CICS transaction name (CTG) equals.

User ID

user

This property only exists if a user ID is set.

Filter: User ID equals.
Requests of the type com.ibm.ctg.client.EPIRequest have the following properties:

Class
The instrumented class com.ibm.ctg.client.JavaGateway

CTG Request Class
  class name
  Default: com.ibm.ctg.client.EPIRequest

CTG Request Type
  EPI

CTG Server name
  server

Method
The instrumented method name is always equal to "flow."

Transaction Name
  transaction ID

User ID
  user
  This property only exists if a user ID is set.
  Filter: User ID equals.
Requests of the type com.ibm.ctg.client.ESIRequest have the following properties:

**Class**
- The instrumented class com.ibm.ctg.client.JavaGateway.

**CTG Request Class**
- *class name*
  - **Default:** com.ibm.ctg.client.ESIRequest

**CTG Request Type**
- ESI

**Method**
- The instrumented method name is always equal to "flow."

**Server Name**
- *server*

**User ID**
- *user*
  - This property only exists if a user ID is set.
  - **Filter:** User ID equals.
Requests of the type com.ibm.ctg.client.XARequest have the following properties:

**Class**

The instrumented class is com.ibm.ctg.client.JavaGateway

**CTG Request Class**

*class name*

*Default:* com.ibm.ctg.client.XARequest

**CTG Request Type**

XA

**Method**

The instrumented method name is always equal to "flow."

**Server Name**

*server*

**User ID**

*user*

This property only exists if a user ID is set.

**XA Request Type**

Has the following values:

- XA_START
- XA_END
- XA_PREPARE
- XA_COMMIT
- XA_ROLLBACK
- XA_FORGET
- XA_RECOVER
- CLEANUP
Blame Point Metrics

The blame point metrics that the CTG CA SYSVIEW Tracer generates are in the following folders, depending on the request type.

- Requests of the type `com.ibm.ctg.client.CicsCpRequest` are in the folder `Backends | CTG Code Page`.
- Requests of the type `com.ibm.ctg.client.ECIRequest` are in the one of the following folders:
  - `Backends | CTG ECI server server program program folder`
  - `Backends | CTG ECT server server ECI_COMMIT folder`
  - `Backends | CTG ECI server server ECI_BACKOUT folder`
- Requests of the type `com.ibm.ctg.client.EPIRequest` are in the folder `Backends | CTG EPI server server transaction transaction`.
- Requests of the type `com.ibm.ctg.client.ESIRequest` are in the folder `Backends | CTG ESI server server`.
- Requests of the type `com.ibm.ctg.client.XARequest` are in the folder `Backends | CTG XA server server XA request type with the following XA request types:`
  - `XA_START`
  - `XA_END`
  - `XA_PREPARE`
  - `XA_COMMIT`
  - `XA_ROLLBACK`
  - `XA_FORGET`
  - `XA_RECOVER`
  - `CLEANUP`
- All other request types are in the `Backends | CTG Unknown folder`.

HTTP Transaction Trace Components Properties

The section describes the components and properties added to Java traces by the HTTP CA SYSVIEW Tracer. Each of the transaction trace components and its properties are described.
HTTP Servlet Tracing Properties

Any subclass of HTTPServlet will generate the HTTP Servlet component when one of the methods that implements methods doGet(), doPut(), doPost() or doDelete() is called. Properties that can be filtered in the Transaction Trace Session dialog box list the filter name.

Class

Identifies the class that implemented the HTTPServlet class.

CrossProcessData

Specifies a UUID used for correlation and is applicable only to HTTP transaction tracers.

This property appears only if this component is the root component.

Format: A 32-byte UUID

Communication Method

Identifies the communication method that is used to invoke the transaction. This value is always set to HTTP.

Filter: CICS/IMS communication method equals

Method

Identifies the called method that was instrumented and which caused the component to be inserted.

Values: doGet, doPut, doPost, and DoDelete

SeqNoCrossProcessData

Specifies the sequence ID of the correlation UUID.

This property appears only if this component is the root component.

Trace ID

Specifies the trace identifier, a unique value that is generated for each trace event.

This property appears only if this component is the root component.
**Trace Type**

Specifies the transaction trace type.

This property appears only if this component is the root component.

**Normal**

Indicates a normal trace that is taken during a transaction trace session.

Alternately, a trace that correlates with a sample from another agent.

**Sampled**

Indicates a sample trace that is taken because sampling is set. The sample trace appears in the Transaction Trace Viewer pane as correlated traces.
URL

Indicates the URL of the servlet. The leading protocol specifier, computer name, and port number are not included.

**Example:** /HTTPTest/servlet/FrontEndClient

**Filter:** URL (from the drop-down list)
URL Connection Tracing Properties

This section lists all of the properties of the URLConnection Tracing component. Any subclass of URLConnection or HttpURLConnection generates the URLConnection Tracing component when the method that implements setDoOutput() is called. Properties that can be filtered in the Transaction Trace Session dialog list the filter name.

**Class**

Identifies the class that implemented the URLConnection or HttpURLConnection class.

**Communication Method**

Identifies the communication method that is used to invoke the transaction. This value is always HTTP.

**Filter**: CICS/IMS communication method equals

**Method**

Identifies the called method that was instrumented and which caused the component to be inserted. This value is always setDoOutput.

**URL**

Displays the URL being invoked. The leading protocol specifier, computer name, and port number are not included.

**Example**: /CICS/CWBA/DFJ$JWB1

**Filter**: URL (from the drop-down list)

![Example Visualization]

- **Agent**: SuperDomain
t- **Timestamp**: 08/03/21 2:15:31 EDT
- **Duration**: 49 ms
- **Component Details**
  - **Type**: URL Connection Tracing
  - **Name**: URL Connection Tracing
  - **Path**: URL Connection Tracing
- **Performance**
  - **Duration**: 0 ms
  - **Timestamp (relative)**: 0 ms
  - 0% of total transaction time
- **Properties**
  - **Class**: sun.net.www.protocol.http.HttpURLConnection
  - **Communication Method**: HTTP
  - **Method**: setDoOutput
  - **URL**: /CICS/CWBA/DFJ$JWB1
Review or Adjust Results Components

The section describes the mainframe transaction trace components and properties the Cross-Enterprise APM agent generates for the mainframe transactions.

The transaction traces are built from standard performance information in the SMF records generated by CA SYSVIEW. The transaction traces consist of a series of components that help you diagnose problems. Each component has properties with names and values.

Some components are permanent and appear in every trace, while others are optional to reduce the size of the traces. These optional components appear in the trace only if they are in one of these two sets:

- The top ten longest non-zero duration components
- Components whose duration is greater than five percent of their parent component

CICS Transaction Tracing

Transactions that run on a CICS region that have been traced generate a minimum of one CICS transaction trace in the workstation. That transaction trace, the CICS Suspend/Dispatch transaction trace, contains suspend and dispatch timings. If any program participating in the transaction calls DB2, then a second transaction trace, the CICS DB2 transaction trace, is generated with DB2 timings.

CICS Transaction Lifetime Component Properties

This section lists all of the properties of the CICS transaction lifetime component. CICS transaction lifetime is the root component of every CICS transaction trace, and any of its child components are nested within it. Properties that can be filtered in the Transaction Trace Session dialog list the filter name.

**ABEND Code**

An ABEND code appears in the bottom pane of the Trace View only when a transaction ends abnormally.

**Applid**

Specifies the network ID of the target CICS server.

**Format:** A string up to eight characters in length

**CrossProcessData**

Specifies a UUID used for correlation and is applicable only to web service transaction tracers.

**Format:** A 32-byte UUID
**Communication Method**

The communication method that is used to invoke the transaction:

- Web Service
- CTG Channel
- MQ Trigger Message
- HTTP

*Filter: CICS/IMS communication method equals*

**IscopeMQID**

Specifies a 48-byte hexadecimal string that is used for the correlation with multiple UUIDs; used with the WebSphere MQ series tracer only. The name and value are reversed for performance improvements on correlation.

**IscopeCTGID**

Specifies a 32-byte UUID used for the correlation with only one UUID; used with the CTG CA SYSVIEW tracers only. The name and value are reversed for performance improvements on correlation.

**Job Name (Server Name)**

Indicates the region where the CICS transaction was processed.

*Filter: CICS server name (CTG) equals*

**Microsecond Lifetime**

Specifies the transaction duration in microseconds.

*Filter: CICS/IMS transaction lifetime lasting longer than*

**Program Name**

Displays the name of the last executed program in the CICS region. If more than one program was run in an extended transaction, then one component per program is a child of the dispatch component. Each child component has a Program Name property listing the associated program.

*Filter: CICS program name (CTG) equals*

**SMF SysId**

Specifies the identifier of the system delivering the SMF records.

**SeqNoCrossProcessData**

Specifies the sequence ID of the correlation UUID.

**Task Number**

Specifies the number that identifies this transaction task.
Trace ID
Specifies the trace identifier, a unique value that is generated for each trace event.

Trace Type
Specifies the transaction trace type.

Normal
A normal trace that is taken during a transaction trace session.
Alternately, a trace that correlates with a sample from another agent.

Sampled
A sample trace that is taken because sampling is set. The sample trace appears in the Transaction Trace Viewer pane as correlated traces.

Transaction Name
Indicates the name of the transaction in the CICS region.

Filter: CICS transaction name (CTG) equals

Transaction Processor
Specifies the transaction processor that ran the transaction.

CICS
Transaction was run on CICS.
Filter: CICS/IMS transaction processor name equals

Umbrella Name
Specifies the transaction ID of the umbrella transaction when it invokes this transaction.

Umbrella Type
The type of the umbrella transaction if present.

Unit of Work ID
Specifies the unit of work ID associated with the transaction.

When the CICS transaction is an issue, use the contents of this field to find the associated SMF record in CA SYSVIEW.

CICS transactions:
CTRANLOG; SELECT UOWID EQ <value_of_Unit_of_Work_ID>;

Note: The CA SYSVIEW administrators can find the corresponding SMF record for this transaction using the CA SYSVIEW GUI.
Web Service Name

Indicates the name of the web service that is used to execute this transaction. This property is applicable only to web service transaction tracers.

Filter: CICS web service name equals

CICS Dispatch Time Component Properties

CICS Dispatch Time is a child component of the CICS Transaction Lifetime root component. Dispatch time contains a single property:

CPU Time

Specifies the portion of dispatch time when the task is using processor cycles.

CICS Suspend Time Component Properties

CICS Suspend Time is a child component of the CICS Transaction Lifetime root component. Suspend time contains these properties:

CICS Exceptions Wait Time

Specifies the accumulated wait time from all the exception conditions.

Java Suspend Time

Specifies the elapsed time over which the CICS dispatcher domain suspends the user task while running in the CICS Java Virtual Machine (JVM).

Java Time

Specifies the total elapsed time that the user task spent in the CICS Java Virtual Machine (JVM)

Max Hot-Pooling TCB Delay Time

Specifies the elapsed time the user task waited to obtain a CICS Hot-Pooling TCB (H8 mode). The MAXHPTCBS system parameter sets the time limit that the CICS system can wait. The HPJ-compiled Java programs that are defined with HOTPOOL(YES) use the H8 mode open TCB exclusively.

QR TCB Wait For Dispatch

Specifies the elapsed time the user task waited for the CICS QR mode TCB to dispatch the task again. QR TCB Wait For Dispatch is defined as aggregate wait times between the following events:

- Wait event completes.
- CICS dispatcher domain on the QR mode TCB dispatches the user task again.
Waiting To Run Time

Specifies the elapsed time the user task waited for the CICS dispatcher domain to dispatch the task again. Waiting To Run Time is defined as aggregate wait times between the following events:

■ Wait event completes.
■ CICS dispatcher domain dispatches the user task again.

Other optional child components appear under Suspend Time if they:

■ Represent a portion of the suspend time.
■ Use non-zero time.
■ Are in the top ten components by usage.
■ Represent more than 5 percent of the Transaction Lifetime.
CICS DB2 Statement Component Properties

This section lists all of the properties of the CICS DB2 statement component.

**Average Time**

Specifies the average time spent executing the DB2 statement. This column is calculated from Total Time/Request Count.

**Program Name**

Specifies the name of the program that executed the DB2 statement.

**Maximum Time**

Specifies the maximum time spent on a single run of a DB2 statement represented by the component. The time includes both suspend and dispatch timings.

**Request Count**

Specifies the number of times that the DB2 statement was executed by the program from that line number. If statement numbers are disabled, it will be the number of times that any DB2 statement of that type was executed from anywhere in the program. If the program ran multiple times within a transaction, then this value is cumulative.

**SSID**

Specifies the subsystem ID on which the DB2 statements were executed.

**Statement Number**

Specifies the numbers that are generated by the DB2 precompiler. This property only exists if CA-SYSVIEW is configured to generate statement numbers.

**Statement Type**

Specifies the type of statement such as SELECT, INSERT, DELETE, or FETCH.

**Note:** You can find a complete list of statements in the *IBM DB2 10 for z/OS SQL Reference*.

**Total Time**

Specifies the total time spent on all of the executed DB2 statements that are represented by the component. The time includes both suspend and dispatch timings.
IMS Transaction Lifetime Component Properties

This section lists all the properties of the IMS Transaction Lifetime component. IMS Transaction Lifetime is the root component of every IMS transaction trace, and any of its child components are nested within it. Properties that can be filtered in the Transaction Trace Session dialog list the filter name.

ABEND Code
Displays the ABEND code when a transaction ends abnormally. The code, if displayed, appears on the bottom pane of the Trace View.

Communication Method
Specifies the communication method that is used to invoke the transaction:

- MQ IMS Bridge
- MQ IMS Adapter

Filter: CICS/IMS communication method equals

CPU Time
Specifies the CPU time the dependent region uses to process the transaction in microseconds. The percentage of the spent Transaction Lifetime or Process time on the CPU is displayed in parentheses.

IscopeMQID
Specifies a 48-byte hexadecimal string that is used for the correlation with multiple UUIDs; used with WebSphere MQ series tracers only. The name and value are reversed for performance improvements on correlation.

Job Name (Dependent Region)
Specifies the dependent region job name of the IMS-dependent region that processed the transaction.

Filter: IMS job name equals

LTerm Name
Specifies the logical terminal name that is associated with this instance of the transaction.

Microsecond Lifetime
Specifies the duration of the Transaction Lifetime in microseconds.

Filter: CICS/IMS transaction lifetime lasting longer than

PSB Name
Specifies the program specification block (PSB) name that is associated with the transaction.

Filter: IMS PSB name equals
Region ID

Specifies the PST ID associated with the IMS-dependent region that processed the transaction.

Trace Type

Specifies the transaction trace type.

Normal

Indicates that a normal trace is taken during a transaction trace session.

Alternately, a trace that correlates with a sample from another agent.

Sample

Indicates that a sample trace is taken because sampling is set. The sample trace appears on the Transaction Trace Viewer pane as correlated traces.

Transaction Class

Specifies the transaction class where the transaction was scheduled.

Transaction ID

Specifies the transaction name

Filter: IMS transaction ID equals

Transaction Origin

Specifies the origin which can be either Shared Queues, OTMA, APPC, LOCAL, or the bit settings in the record description.

Transaction Priority

Specifies the priority at which the transaction was dispatched.

Transaction Processor

Specifies the transaction processor that ran the transaction.

IMS

Transaction was run on IMS.

Filter: CICS/IMS transaction processor name equals
**Transaction Type**

Specifies the transaction types.

- A - Program ABEND
- B - Processing restarted
- C - Conversational send/receive
- D - Transmit only conversations
- F - FORMAT entered
- M - Message switch
- O - Region Occupancy
- P - Program switch
- Q - Transmit only program switch
- R - Program running at ABEND
- S - Send/Receive processing
- T - Transmit only
- X - Conversational program switch
- Y - Transmit only conversational program switch
- Z - Transaction IMLB time-out

**Unit of Work ID**

Specifies the unit of work ID associated with the transaction.

Use the contents of this field to find the associated SMF record in CA SYSVIEW.

IMS transactions:

IMSTLOG UOW <value_of_Unit_of_Work_ID>;

**User ID**

Specifies the user ID associated with this instance of the transaction.

**Filter:** user ID
IMS Optional Component Properties

This section lists all IMS optional component properties. These are optional properties of the Process Time child component. Process Time is a child component of the IMS transaction lifetime root component. The Optional Components are IMS Monitor type events such as, IWAITs, DL/1 and External Subsystem calls that occur during the transaction lifetime. There is only a single component for each event type. These properties exist only if more than one event has occurred.

**Event Count**

Specifies the number of times the event occurred during the processing of the transaction.

**Maximum Event Time**

Specifies the longest duration of any event of this type.

IMS Process Time Component Properties

This section lists all properties of the IMS Process Time child component. Process Time is a child component of the IMS transaction lifetime root component.

**CPU Time**

Specifies the CPU time the dependent region uses to process the transaction in microseconds. The percentage of the Process Time spent on CPU is displayed in parentheses.
Chapter 5: CA APM Cross-Enterprise Metrics

This section contains the following topics:

About CTG CA SYSVIEW Tracer Metrics (see page 143)
About CA Cross-Enterprise APM z/OS Metrics (see page 144)
CA SYSVIEW Metric Categories (see page 145)
DB2 z/OS Subsystems Metrics (see page 184)
CA NetMaster NM for TCP/IP Metric Categories (see page 196)

About CTG CA SYSVIEW Tracer Metrics

With the CTG CA SYSVIEW tracer, you receive metrics concerning CTG calls made by the application that was instrumented with the tracer. These blame-point metrics are known as backends of the front-end metrics. They also appear on the triage map.

The back-end metrics for the sockets (host/port pairs) used to communicate with the CTG server also appear. The CTG back-end metrics also appear under Called Backends for any front ends that call it.

Participation in the Application Map is as a back end with the same naming convention for the vertex.
On the Workstation Triage Map, you can view the back end by selecting the front end that calls it. A front end must be generated to see this back end. Some pbd must define front-end metrics for some method that in turn calls the method `com.ibm.ctg.client.JavaGateway.flow()`.

The circular green icons (at which the arrows point) indicate that metrics exist. These metric icons can be used to access blame point metrics for the call to the method `com.ibm.ctg.client.JavaGateway.flow()`. These metric icons appear only when the application is up and the agent is connected to the EM. Mouse over the metric icon, and the metrics appear.

About CA Cross-Enterprise APM z/OS Metrics

Use the CA APM Cross-Enterprise metrics to identify problems. They can be viewed in the CA Introscope® Workstation.

**Note:** For more information about the GC Heap and Host metrics, see the CA APM Workstation User Guide. You can access this guide from the CA Technical Support site.
CA SYSVIEW Metric Categories

You can configure the CA Cross-Enterprise APM Agent to collect metrics from a single instance of CA SYSVIEW. The agent must be running on the same LPAR as that instance is running.

The configuration file, Cross-Enterprise_APM_Dynamic.properties, has configuration properties for the collection (yes, no) or regex (regular expression) for each metric category. The properties that end with ‘.collect’ control whether the associated CA SYSVIEW command is executed at all. The properties that end with ‘.regex’ can be set to the following values:

- Blank to prevent the collection
- Regular expression to filter the queue managers, queues, address spaces, subsystems, or regions to collect

Within the regex value, you can also use selection criteria wildcards. For example, regex=CQ* gathers only those regions beginning with the letters CQ.

If the collection for a metric category is enabled, then you can also specify the frequency of collection using the skip interval properties.

The configuration file has specific examples and helping instructions that are contained within the file.

Each monitored CA SYSVIEW subsystem reports metrics. The metric categories are as follows:

**z/OS Metrics** *(see page 149)*

Folders:

- z/OS Metrics
- z/OS Metrics|Paging
- z/OS Metrics|Processor
- z/OS Metrics|Status
- z/OS Storage

Configuration properties:

- SYSVIEW.ZOS.Metrics.collect=yes
- SYSVIEW.ZOS.Skip.Intervals=0

**z/OS Alerts** *(see page 153)*

Folders:

- z/OS Metrics|Alerts
Configuration properties:

- SYSVIEW.ZOS.Alerts.Metrics.collect=yes
- SYSVIEW.ZOS.Alerts.Skip.Intervals=0

**z/OS Degradation Delay Analysis** *(see page 155)*

Folders:
- z/OS Metrics|Degradation Delay Analysis

Configuration properties:

- SYSVIEW.ZOS.Delays.Metrics.collect=yes
- SYSVIEW.ZOS.Delays.Skip.Intervals=0

**z/OS Workload Manager Service Goals** *(see page 158)*

Folders:
- z/OS Metrics|Workload Manager Service Goals

Configuration properties:

- SYSVIEW.ZOS.WLM.Metrics.collect=yes
- SYSVIEW.ZOS.WLM.Skip.Intervals=0

**CICS Regions** *(see page 160)*

Folders:

- CICS Regions|<region name>
- CICS Regions|<region name>|Dynamic Storage Area
- CICS Regions|<region name>|Status

Configuration properties:

- SYSVIEW.CICS.Regions.regex=*  
- SYSVIEW.CICS.Skip.Intervals=0

**CICS Transaction Groups** *(see page 163)*

Folders:

- CICS Regions|<region name>|Transaction Groups|<Group name>

Configuration properties:

- SYSVIEW.CICS.TransactionGroups.regex=*  
- SYSVIEW.CICS.Skip.Intervals=0
CICS Alerts (see page 164)

Folders:
- CICS Regions
  - Metrics
    - Unacknowledged Alert Count
    - Unacknowledged Problem Count
- CICS Regions |<region name>|Alerts

Configuration properties:
- SYSVIEW.CICS.Alerts.Regions.regex=*  
- SYSVIEW.CICS.Alerts.Skip.Intervals=0

CICS Degradation Analysis (see page 166)

Folders:
- CICS Regions |<region name>|Degradation Analysis |<Resource>

Configuration properties:
- SYSVIEW.CICS.Degradation.Regions.regex=*  
- SYSVIEW.CICS.Degradation.Skip.Intervals=0

DATACOM Address Spaces (see page 167)

Folders:
- DATACOM Address Spaces |<address space name>

Configuration properties:
- SYSVIEW.Datacom.Address.Space.regex=*  
- SYSVIEW.Datacom.Address.Space.Skip.Intervals=0

IMS Subsystems (see page 170)

Folders:
- IMS Subsystems |<subsystem name>
- IMS Subsystems |<subsystem name> |Configuration Properties
- IMS Subsystems |<subsystem name> |Status

Configuration properties:
- SYSVIEW.IMS.Subsystem.regex=*  
- SYSVIEW.IMS.Subsystem.Skip.Intervals=0
**IMS Transaction Groups** *(see page 172)*

Folders:
- IMS Subsystems | <subsystem name> | Transaction Groups | <group name>

Configuration properties:
- SYSVIEW.IMS.TransactionGroups.regex=*
- SYSVIEW.IMS.Subsystem.Skip.Intervals=0

**MQ Queue Managers** *(see page 173)*

Folders:
- MQ Queue Managers
- MQ Queue Managers | <queue manager name> | Configuration Properties
- MQ Queue Managers | <queue manager name> | Status
- MQ Queue Managers | <queue manager name> | Queues [partial control]

Configuration properties:
- SYSVIEW.MQ.QMs.regex=*
- SYSVIEW.MQ.Skip.Intervals=0

**MQ Alerts** *(see page 177)*

Folders:
- MQ Queue Managers
  - Metrics
    - Unacknowledged Alert Count
    - Unacknowledged Problem Count
- MQ Queue Managers | <queue manager name> | Alerts

Configuration Properties:
- SYSVIEW.MQ.Alerts.QMs.regex=*
- SYSVIEW.MQ.Alerts.Skip.Intervals=0

**MQ Queues** *(see page 178)*

Folders:
- MQ Queue Managers | <queue manager name> | Queues
- MQ Queue Managers | <queue manager name> | Queues | <queue name> | Configuration Properties
- MQ Queue Managers | <queue manager name> | Queues | <queue name> | Status
Configuration properties:
- SYSVIEW.MQ.Queues.regex=*  
- SYSVIEW.MQ.Skip.Intervals=0

**TCP/IP Stacks (see page 181)**

Folders:
- TCPIP Stacks|<stack>
- TCPIP Stacks|<stack>|Status

Configuration properties:
- SYSVIEW.TCPIP.Stack.regex=*  
- SYSVIEW.TCPIP.Stack.Skip.Intervals=0

---

**z/OS Metrics**

CA APM Cross-Enterprise monitors data for the z/OS metrics.

The z/OS metrics appear under the folder: z/OS Metrics.

Additionally, the following z/OS-related data is reported in subfolders:
- **Paging** (see page 150)
- **Processor** (see page 150)
- **Status (z/OS Metrics)** (see page 151)
- **Storage** (see page 152)

These z/OS metrics are in the z/OS metrics folder:

**IO Rate Per Second**

(Disk I/O only) Displays the number of start I/Os per second for the system.

**LPAR Name**

Displays the name of the LPAR.

**Spool Utilization (%)**

Displays the indication of spool utilization.

*Print spool %*

**Tasks Ready To Dispatch**

Displays the number of tasks that are ready to dispatch.
Paging

The z/OS paging metrics appear under the folder: z/OS Metrics | Paging.

These paging metrics are reported for z/OS:

**Available Frame Queue Average**
- Displays the average of the available frame queue.

**Local Page Dataset Slots In Use (%)**
- Displays the percentage of local page data set slots in use.

**Paging Per Second**
- Displays the paging rate per second for the system.

**Unreferenced Interval Count Average**
- Displays the average of unreferenced interval counts.

Processor

The z/OS processor metrics appear under the folder: z/OS Metrics | Processor.

These processor metrics are reported for z/OS.

**CP (%)**
- Displays the percentage of busy CPU from a z/OS point of view. This includes only CP processors.

**CPU (%)**
- Displays the percentage of busy CPU from a z/OS point of view. This includes all processors.

**IFA (%)**
- Displays the percentage of busy CPU from a z/OS point of view. This includes only IFA processors.

**IIP (%)**
- Displays the percentage of busy CPU from a z/OS point of view. This includes only IIP processors.

**LPAR CP (%)**
- Displays the percentage of busy CPU from a LPAR point of view. This includes only CP processors.

**LPAR CPU (%)**
- Displays the percentage of busy CPU from a LPAR point of view. This includes all processors.
LPAR IFA (%)
Displays the percentage of busy CPU from a LPAR point of view. This includes only IFA processors.

LPAR IIP (%)
Displays the percentage of busy CPU from a LPAR point of view. This includes only IIP processors.

Status (z/OS Metrics)
The z/OS status metrics appear under the folder: z/OS Metrics | Status.

These status metrics are reported for z/OS:

**Dump Data Sets**
Indicates a dump data set is in use.

**Enqueue Conflicts**
Indicates a potential enqueue conflict could exist.

**Enqueue Reserves**
Indicates a potential enqueue reserve problem could exist. If this value is blank, it indicates no problem exists.

**LPAR**
Displays the LPAR with these values.

1
ACTIVE

0
All values except ACTIVE (that is, NO_COMM or NO_SRVR)

**SMF**
Indicates a potential SMF problem could exist with these values.

0
If the field is blank, no problem exists.

1
The field has the same value as the metric, which means a problem exists. In this case, the value would be SMF for a problem.
**Tape Mounts**

Indicates a tape mount is pending with these values.

0

If the field is blank, no problem exists.

1

The field has the same value as the metric, which means a problem exists. In this case, the value would be TAP for a problem.

**WTO**

Indicates a potential WTO problem could exist with these values.

0

If the field is blank, no problem exists.

1

The field has the same value as the metric, which means a problem exists. In this case, the value would be WTO for a problem.

**Storage**

The z/OS storage metrics appear under the folder: z/OS Metrics|Storage.

These storage metrics are reported for z/OS.

**Common Storage Area (CSA %)**

Displays the percentage of common storage area in use.

**Extended Storage Area (ECSA %)**

Displays the percentage of extended common storage area in use.

**Extended System Queue Area (ESQA %)**

Displays the percentage of extended system queue area in use.

**System Queue Area (SQA %)**

Displays the percentage of system queue area in use.
z/OS Alerts

All metrics are reported on every polling interval unless the alert has been acknowledged, in which case, the metrics are absent and they go gray.

Only the alerts that are unacknowledged appear in the Workstation Investigator tree. Metrics appear under the z/OS Metrics|Alerts folder, which give total counts of these unacknowledged alerts. If you want alerting on the CA SYSVIEW z/OS alert activity, use these metrics to generate the APM alerts through the management module editor.

**z/OS Metrics|Alerts: Unacknowledged Problem Count**

The current number of alerts that have a status of problem.

**z/OS Metrics|Alerts: Unacknowledged Alert Count**

The current number of unacknowledged alerts.

**z/OS Metrics|Alerts: Unacknowledged Warning Count**

The current number of MQ alerts that have a status of warning.

The metrics for each z/OS alert appear under the folder: z/OS Metrics|Alerts|<Alert Name>_<Resource Name>_<Alias Name>.

**Alert Name**

The name of the alert. In CA SYSVIEW, it is the variable name for the data collection element of the alert. This metric is the prefix of the folder name for the alert.

**Alert Status**

The current alert threshold status. This value can be NONE, NORMAL, HIGH, WARNING, or PROBLEM.

**Alert Status Value**

The current alert threshold status as a numeric value. This value can be 0=NONE, 1=NORMAL, 2=HIGH, 3=WARNING, or 4=PROBLEM.

**Alias**

The alias of the alert. In CA SYSVIEW, it is the alias for the resource argument. This metric is absent if it has no value. This value becomes the third underscore separated segment of the metric folder name for the alert when it exists.

**Description**

A description of the alert.

**Group**

A group classification for the alert.

**Priority**

The priority of the alert from 0 through 999 with 999 having the highest priority.
**Resource Name**

The resource of the alert. In CA SYSVIEW, it is the resource argument that is used to qualify the collection element of the alert. This metric is absent if it has no value. This value becomes the second underscore separated segment of the alert folder name when it exists.

**Rule Type**

The exception rule type. Possible values are:

- **UPPER**—Upper limit threshold
- **LOWER**—Lower limit threshold
- **CHANGE**—Change in the value threshold
- **STATE**—State exception
- **SUMMARY**—Summarized entry

**Value**

The value last used during threshold processing. If the resource does not currently have an associated threshold definition, the value is the last value the data Collector collects.
The `typeview` on the `z/OS Metrics` folder tab `Alerts` has the following display:

- Unacknowledged alert, problem, and warning count on a single graph at the top
- Individual alerts in the table at the bottom

Similarly, the `typeview` also displays on the `Alerts` folder tab `Overview`. The columns are sorted on `Priority` and then `Status`. In this way, the highest priority items appear at the top of the list with the highest status of those items first. The status value column is color-coded to severity with `Red = Problem` and `Yellow = Warning`. Selecting the `z/OS Metrics | Alerts` folder tab `Overview` brings up the identical `typeview`.

---

**z/OS Degradation Delay Analysis**

Degradation delay metrics will appear only for the top 20 worst `Job Nameigraphy ASID` as determined by the delay percent value. If a job is no longer within the top 20, the metrics will not be reported; the metrics will be absent and the job name will change to gray.

The metrics for each degradation delay appear under the folder: `z/OS Metrics | Degradation Delay Analysis|<Job Name>_<ASID>`. 
These metrics are listed in the order they appear on the Degradation Delay Analysis Typeview table and so are not in alphabetical order.

**Job Name**

Specifies the name of the job. The value of this metric forms the first part of the degradation delay's folder name.

**ASID**

Specifies the hexadecimal address space ID. This metric will not appear if it has no value. This becomes the second underscore separated segment of the degradation delay's folder name when it exists.

**Reason**

Specifies the reason for the delay. The value of this metric determines how the ‘Detail’ metric should be interpreted. This table lists the possible reasons and the meaning of the details provided.

<table>
<thead>
<tr>
<th>Reason</th>
<th>Explanation of the delay</th>
<th>The 'Detail' metric provides</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>CPU time was not available</td>
<td>The top five users upon which the CPU resources were waiting. It is possible for a multi-T CB ASIC to be waiting on itself.</td>
</tr>
<tr>
<td>DEVICE</td>
<td>Device(s) were not available</td>
<td>The top six devices upon which the job was waiting.</td>
</tr>
<tr>
<td>STORAGE</td>
<td>Storage was not available</td>
<td>No additional details are available.</td>
</tr>
</tbody>
</table>

**JES**

JES resources were not available

**JES2 Code Explanation:**

- 0001 - Processing TSO OUTPUT command request
- 0002 - Waiting for JES2 to cancel a job
- 0003 - Waiting for job status information from JES2
- 0012 - Waiting for JES2 to purge a SYSOUT file
- 0013 - Waiting for JES2 to restart a job

**JES3 Code Explanation:**

- 0023 - Dynamically allocating data set to JES3
- 0026 - Changing DDNAME of device or data set
- 0027 - Changing data set use from SHR to OLD
- 0132 - Allocate or deallocate spool data set
Reason | Explanation of the delay | The 'Detail' metric provides
---|---|---
HSM | HSM resources were not available | **Code Explanation**
|  | 03 - A data set is being recalled from auxiliary storage
|  | 05 - A data set is being recovered
|  | 06 - A data set is being migrated
|  | 07 - A data set is being backed up
|  | 08 - A control data set record is being read, or a JES3 C/I locate is being done
|  | 12 - A data set is being deleted
XCF | XCF resources were not available | No additional details are available.
MOUNT | A device was waiting to be mounted | VOLSER waiting to be mounted.
MESSAGE | An operator reply was pending | The operator reply number.
ENQUEUE | An enqueue conflict exists | The QNAME:RNAME of the enqueue.

**CPU**
Specifies the percent of time the job was waiting for CPU resources during the interval.

**Device**
Specifies the percent of time the job was waiting for a device during the interval.

**Storage**
Specifies the percent of time the job was waiting for storage during the interval.

**Subsystem**
Specifies the percent of time the job was waiting for a subsystem request during the interval.

**Operator**
Specifies the percent of time the job was waiting for an operator response during the interval.

**Enqueue**
Specifies the percent of time the job was waiting for access to an enqueue during the interval.
Delay Percent

Specifies the percent of time the job was waiting for resources during the interval. On the typeview Degradation Delay Analysis table this field will highlight yellow to indicate warning if it is 50 percent or greater but less than 75 percent. It will highlight red to indicate problem if the percent is 75 percent or more. The typeview threshold values for the warning and problem status modes are not modifiable.

Detail

See the detail supplied in the table for the Reason metric.

The typeview on the z/OS Metrics folder tab Degradation Delay Analysis displays all the individual degradation delays. The Degradation Delay Analysis displays all the individual delays in a single table. The columns appear in the general order as the CA SYSVIEW delays display; with the different that ASID will be displayed to the immediate right of the Job Name and several other fields are not displayed. The rows are sorted on the Delay Percent column, so that the most delayed items appear at the top and the highest status is first. The Delay Percent column will be color coded as to severity with Red indicating greater than 75% delay and yellow indicating greater than 50% delay. This typeview is also available by selecting the z/OS Metrics|Degradation Delay Analysis folder in the tree and tab Overview in the right hand panel.

z/OS Workload Manager Service Goals

The workload manager metrics appear in the investigator tree under the folder Workload Manager Service Goals, which is inside the z/OS Metrics folder. Each service goal has one subfolder using the Workload_Class_Period triplet as the name. The three part folder name uses underscore separators between Workload, Class, and Period.

They all appear under the folder: z/OS Metrics|Workload Manager Service Goals|<Workload>_<Class>_<Period>.

Workload

Displays the name of the workload that is associated with this service class.

Class

Displays the service class name.

Period

Displays the period number.

Importance

Displays the importance level ranging from 1 to 5, where 1 is most important. For discretionary goal types, the character 'D' is displayed.
Index
Displays the performance index. The condition level is set based on the following rules:

<table>
<thead>
<tr>
<th>Index</th>
<th>Importance</th>
<th>Condition</th>
<th>Index Value</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater than 1.0</td>
<td>1, 2</td>
<td>Problem</td>
<td>4</td>
<td>Red</td>
</tr>
<tr>
<td>Greater than 1.0</td>
<td>3, 4, 5, D</td>
<td>Warning</td>
<td>3</td>
<td>Yellow</td>
</tr>
<tr>
<td>Less than or equal to 1.0</td>
<td>any</td>
<td>Normal</td>
<td>1</td>
<td>None</td>
</tr>
<tr>
<td>Equal to 0 (zero)</td>
<td>any</td>
<td>None</td>
<td>0</td>
<td>None</td>
</tr>
</tbody>
</table>

Index Value
Displays the index condition value. Values are 0 = none, 1 = normal, 2 = warning, and 3 = problem.

Goal Type
Displays the goal type. Possible values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESPPCT</td>
<td>Response time percent</td>
</tr>
<tr>
<td>RESP AVG</td>
<td>Response time average</td>
</tr>
<tr>
<td>VELOCITY</td>
<td>Velocity</td>
</tr>
<tr>
<td>DISCRETE</td>
<td>Discrete</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>System</td>
</tr>
</tbody>
</table>

The typeview on the z/OS Metrics folder tab Workload Manager Service Goals displays all individual workload manager service goals. The rows are sorted on Index Value so that the service goals most in threat appears at the top of the table. The Index Value column is color-coded as to severity with red indicating problem and yellow indicating warning.
CICS Regions

CA APM Cross-Enterprise monitors data for the CICS regions that are configured for your environment. For more information about configuring the CICS regions, see Configure the Cross-Enterprise_APM_Dynamic.properties File (see page 38).

The CICS Regions metrics appear under the folders (one for each region): CICS Regions|<region name>.

Additionally, the following CICS regions-related data is reported in subfolders:
- Dynamic storage area (see page 163)
- Status (see page 160)
- Transaction groups (see page 163)

The following metrics are for the CICS regions:

**Average CPU Time Per Transaction (µs)**
- Specifies the average CPU time per transaction in microseconds.

**Average Lifetime Per Transaction (µs)**
- Specifies the average lifetime per transaction response time in microseconds.

**Average Suspend Time Per Transaction (µs)**
- Specifies the average suspend time per transaction per second in microseconds.

**Average Time Spent On File Control (µs)**
- Specifies the average time spent doing file control in microseconds.

**Average Waiting To Run Time (µs)**
- Specifies the average time waiting to run time in microseconds.

**Number of Transactions**
- Specifies the number of transactions since the monitor has been running.

**Transactions Per Second**
- Specifies the number of transactions per second.

**Status (CICS Regions)**

The CICS regions status metrics appear under the folder: CICS Regions|<region name>|Status.

These status metrics are reported for CICS regions. For the status metrics, every field from CA SYSVIEW is displayed as two metrics.
The first metric without the value suffix shows the actual status as a string. The possible values vary from one metric to another.

The second metric with the value suffix shows a numeric value for the status of the metric. This one applies to all status metrics. The CICS metrics usually have the same mapping.

Possible values are:
- 0 is NONE.
- 1 is NORMAL.
- 2 is HIGH.
- 3 is WARNING.
- 4 is PROBLEM.

The following status metrics are available:

**DB Control Connection**
Displays the database control connection status.

**DB Control Connection Value**
Displays the value of the database control connection status. The values are.
- Connected
- None

**DB2 Connection**
Displays the database connection status.

**DB2 Connection Value**
Displays the value of the database connection status. The values are.
- Connected
- None

**Maximum CICS Task**
Displays the status indicator for the maximum CICS task status.

**Maximum CICS Task Value**
Displays the value of the maximum CICS task status.
Region Monitoring
Displays the CICS region. Region Monitoring shows the actual values which are:

Active
Indicates that the CICS monitor is active.

Cancelled
Indicates that the address space has been canceled and monitoring is terminated.

Inactive
Indicates that the CICS monitor is inactive.

Nostart
Indicates that the CICS monitor has never been started within this CICS region. The product is probably not installed in the region.

Restart
Indicates that you have to restart the CICS monitor. In most cases, this condition is due to the CICS region terminating abnormally. The CICS monitor was not able to terminate properly. Restart the CICS monitor by using the INIT line command or execute the CICS transaction XPFS from within the CICS address space.

Region Monitoring Value
Displays the value of the CICS Region Monitoring.

Region Status
Displays the maximum of any of the other CICS status values (except the region monitoring value) as a string:

Value: None, Normal, High, Warning, or Problem

Region Status Value
Displays the maximum value of any CICS region status.

TCPIP Connection
Displays the status of the TCPIP connection.

TCPIP Connection Value
Displays the value of the TCPIP connection.

VTAM Connection
Displays the status of the VTAM connection.

VTAM Connection Value
Displays the value of the VTAM connection.
Web Connection
Displays the status of the web connection.

Web Connection Value
Displays the value of the web connection status.

WebSphere MQ Connection
Displays the status of the WebSphere MQ connection.

WebSphere MQ Connection Value
Displays the value of the WebSphere MQ connection status.

Dynamic Storage Area
The CICS regions dynamic storage area metrics appear under the folder: CICS Regions | <region name> | Dynamic Storage Area.

These dynamic storage area metrics are reported for CICS regions.

Dynamic Storage Area (DSA) Amount Free
Specifies the amount of free dynamic storage area.

Dynamic Storage Area (DSA) Free (%)
Specifies the percentage of free dynamic storage area.

Extended Dynamic Storage Area (EDSA) Amount Free
Specifies the amount of free extended dynamic storage area.

Extended Dynamic Storage Area (EDSA) Free (%)
Specifies the percentage of free extended dynamic storage area.

Global Dynamic Storage Area (GDSA) Amount Free
Specifies the amount of free global dynamic storage area.

Global Dynamic Storage Area (GDSA) Free (%)
Specifies the percentage of free global dynamic storage area.

CICS Transaction Groups
The CICS regions transaction group metrics appear under the folders: CICS Regions |<region name> | Transaction Groups |<Group name>.

Metrics are shown for transactions groups, not individual transactions. The CICS Transaction Groups are defined in CA SYSVIEW.
You can configure what transaction groups are monitored for your environment’s CICS regions. For more information about configuring transaction groups, see Configure the Cross-Enterprise_APM_Dynamic.properties File (see page 38).

These are the metrics shown for each transaction group:

**Average CPU Time (µs)**
Displays the average CPU time used in microseconds.

**Average File Control Time (µs)**
Displays the average file control time in microseconds.

**Average Lifetime (µs)**
Displays the average lifetime of the transaction in microseconds.

**Average Suspend Time (µs)**
Displays the average time spent in a suspended state in microseconds.

**Average Waiting to Run Time (µs)**
Displays the average time spent waiting to run in microseconds.

**Elapsed Time Since the Transaction Last Ran (sec)**
The time elapsed in seconds since the last transaction ran in seconds.

**Executed Transaction Count (This Interval)**
Displays an aggregate of the number of times the transaction executed.

**Last Date Since the Transaction Ran**
Displays the date since the last transaction ran.

**Last Time Since the Transaction Ran**
Displays the time since the last transaction ran.

**Transaction Rate (Last System Interval)**
Displays the transaction rate within the last system interval.

### CICS Alerts

All metrics are reported on every polling interval unless the alert has been acknowledged. In which case the metrics are absent and go gray. CICS Alerts shows partially blank rows when the time range other than current is selected. The feature does not support strings in historical mode.
Only the alerts that are unacknowledged appear in the Workstation Investigator tree. Two metrics appear under the CICS Regions folder, which give total counts of these unacknowledged alerts over all CICS Regions. If you want alerting on the CA SYSVIEW CICS alert activity, use these metrics to generate the APM alerts through the management module editor.

**Unacknowledged Problem Count**

The current number of CICS alerts that have a status of problem.

**Unacknowledged Alert Count**

The current number of unacknowledged CICS alerts.

**Unacknowledged Warning Count**

The current number of CICS alerts that have a status of warning.

The metrics for each CICS alert appear under the folder structure: CICS Regions | <Region> | Alerts | <Name> <Arg1> <Arg 2> <Task>.

**Alert Status**

The current alert threshold status. This value can be NONE, NORMAL, HIGH, WARNING, or PROBLEM.

**Alert Status Value**

The current alert threshold status as a numeric value. This value can be 0=NONE, 1=NORMAL, 2=HIGH, 3=WARNING, or 4=PROBLEM.

**Description**

A description of the alert.

**Job Name**

The CICS Region job name of the owning resource.

**Name**

The name of the alert. In CA SYSVIEW, it is the variable name for the data collection element of the alert. This metric is the prefix of the alert folder name.

**Priority**

The priority of the alert from 0 through 999 with 999 having the highest priority.

**Resource Argument 1/Resource Argument 2**

The first/second resource argument. In CA SYSVIEW, it is the first/second resource argument to qualify the collection element of the alert. This metric does not appear if it has no value. This value becomes the second and third underscore separated segments of the alert folder name when they exist.
Rule Type

The exception rule type. Possible values are:

- UPPER indicates the upper limit threshold.
- LOWER indicates the lower limit threshold.
- CHANGE indicates a change in the value threshold.
- STATE indicates a state exception.

Subgroup

The subgroup classification for the alert.

Task

The task number of the task that is being monitored dynamically. This metric does not appear if it has no value. This value becomes the fourth pound sign (#) separated portion of the alert folder name when it exists.

Value

The value last used during threshold processing. If the resource does not currently have an associated threshold definition, the value is the last value the data collector collects.

CICS Degradation Analysis

CICS Degradation Analysis will show partially blank rows when the time range other than current is selected. This is because it does not support strings in historical mode.

The metrics for each CICS degradation analysis appear under the folder structure:

CICS Regions|<Region>|Degradation Analysis|<Resource>

Average

Displays the average time for each transaction monitored.

Job Name

Specifies the name of the CICS region.

Row

Displays the row number to allow sorting to match how they are presented in CA-SYSVIEW.

Percent

Displays the percent of lifetime spent on this resource activity.

Resource

Displays the name of the resource for which timings were collected.
**Datacom Address Spaces**

Cross-Enterprise APM monitors data for CA Datacom address spaces.

The DATACOM address space metrics appear under the folders (one for each address space): DATACOM Address Spaces|<address space>.

Additionally, the status for CA Datacom address spaces is reported in the alert subfolder. For more information about these metrics, see [Status (Datacom Address Spaces)](see page 168).

These are the status metrics:

- **Amount of Real Storage Used (kb)**
  - Displays the amount of real storage in kilobytes the job is using in the private region.

- **CPU Time Accumulated (µs)**
  - Displays the accumulated CPU time in microseconds used by the job.

- **CPU Time Per Interval (µs)**
  - Displays the accumulated CPU time in microseconds used by the job for the interval specified.

- **Datacom Release**
  - Displays the CA Datacom release.

- **EXCPs Outstanding**
  - Displays the EXCPs outstanding. If this value reaches zero, an SC22 abend occurs.

- **Executed Amount Of Wall Clock Time (sec)**
  - The amount of time it takes the wall clock to execute for the Datacom address space.

- **Executed I/O Operations Count**
  - Displays the number of I/O operations performed by the Datacom address space.

- **Executed I/O Operations Count Per Interval**
  - Displays the number of I/O operations performed by the Datacom address space for the specified interval.

- **SVC Number**
  - Displays the Datacom SVC number as defined in the DBSIDPR module.
SubID
Displays the Datacom SUBID defined in the DBSIDPR module.

System Table Value
Displays the system table value specified in the DATACOM parmlib member. The default value is 1000.

Status (CA Datacom Address Spaces)
The DATACOM address space status metrics appear under the folder: DATACOM Address Spaces\<address space>\Status.

The CA Datacom address spaces status is reported by a severity level status indicator and a symbolic job specifier.

Address Space Value
Displays the values for the severity status indicator. Possible values with descriptions:

- **0 and 1**
  Normal condition

- **2**
  A notification or highlighted condition

- **3**
  A warning condition

- **4**
  A problem or critical condition

Symbolic Job Specifier
Displays the symbolic job specifier. Possible values with descriptions:

- **NS**
  Nonswappable

- **LSW**
  Logically swapped

- **GO OUT**
  Currently being swapped out

- **GO IN**
  Currently being swapped in
IN
  Swapped in

OUT TO
  Swapped out--terminal output wait

OUT TI
  Swapped out--terminal input wait

OUT LW
  Swapped out--long wait

OUT XS
  Swapped out--auxiliary storage shortage

OUT RS
  Swapped out--real storage shortage

OUT DW
  Swapped out--detected wait

OUT RQ
  Swapped out--requested swap

OUT NQ
  Swapped out--enqueue exchange swap

OUT EX
  Swapped out--exchange on recommended value

OUT US
  Swapped out--unilateral swap

OUT TS
  Swapped out--transition swap

OUT IC
  Swapped out--improve central storage

OUT IP
  Swapped out--improve system paging

OUT MR
  Swapped out--make room

OUT AW
  Swapped out--APPC wait
IMS Subsystems

Cross-Enterprise APM monitors data for IMS subsystems.

The IMS Subsystem metrics appear under the folders (one for each subsystem): IMS Subsystems | <subsystem name>.

Additionally, the status for IMS subsystems is reported. For more information about status metrics, see Status (IMS Subsystems) (see page 172).

These are the status metrics:

**Amount Of Real Storage Used (kb)**
Displays the amount of real storage in kilobytes the control region is using in the private region.

**Average CPU Time Per Transaction(µs)**
Displays the CPU time per transaction in microseconds.

**Average Input Queue Time Per Transaction (µs)**
Displays the input queue time in microseconds. This is the time input transactions waited in the input message queue for scheduling. This is an average.

**Average Lifetime per Transaction(µs)**
Displays the sum of inqueue, process and outqueue time. This is the average in microseconds.

**Average Output Queue Time Per Transaction(µs)**
Displays the amount of time transaction output waiting in the message queue before being delivered to its final destination. This is the average in microseconds.
**Average Processing Time Per Transaction (µs)**
Displays the transaction processing time in microseconds. This is the amount of time it took to process the transaction once it’s scheduled. This is an average.

**CPU Time accumulated (µs)**
Displays the accumulated CPU time in CPU microseconds the control region is using in the private region.

**CPU Time Per Interval (µs)**
Displays the accumulated CPU time in CPU microseconds the control region is using in the private region during the last metric polling interval.

**Count of Programs Stopped**
Displays the number of programs that are currently in a stopped state.

**Count of Transactions Stopped**
Displays the number of transactions that are currently in a stopped state.

**Executed I/O Operations Count**
The number of I/O operations performed by the control region.

**Jobname**
Displays the name of the IMS control region.

**Monitored By SYSVIEW**
Indicates whether or not the IMS subsystem is being monitored by CA SYSVIEW. Possible values are:

- **MON**
  The IMS subsystem is being monitored by the product.

- **blank**
  The IMS subsystem is not being monitored by the product.

**Transaction Queue Depth**
Displays the volume of jobs in the IMS transaction queue.

**Transactions Per Second**
Displays the transaction rate per second over the requested interval.

**Transaction Rate Per Interval**
Displays the rate of IMS transactions per CA SYSVIEW monitoring interval.

**Configuration Properties | IMS Subsystem Name**
Displays the IMS subsystem name.
Status (IMS Subsystems)

The status of the IMS subsystems.

The IMS Subsystem status metrics appear under the folder: IMS Subsystems | <subsystem name> | Status.

This metric appears as a string value and numeric status indicator.

Subsystem

Displays the status of the current control region status.

Subsystem Value

Displays the value of the status of the current control region status with these values.

0

NONE

1

NORMAL

2

HIGH

3

WARNING

4

PROBLEM

IMS Transaction Groups

Metrics are shown for transactions groups, not individual transactions. The IMS Transaction Groups are defined in CA SYSVIEW.

The IMS Subsystem transaction groups metrics appear under the folder: IMS Subsystems | <subsystem name> | Transaction Groups | <group name>.

You can configure what transaction groups are monitored for your environment’s IMS subsystem. For more information about configuring transaction groups, see Configure the Cross-Enterprise_APM_Dynamic.properties File (see page 38).
These are the metrics shown for each transaction group:

**Average CPU Time Per Transaction(µs)**
- Displays the CPU time per transaction.

**Average Input Queue Time Per Transaction(µs)**
- Displays the average input queue time. This is the time input transactions waited in the input message queue for scheduling.

**Average Lifetime per Transaction(µs)**
- Displays the sum of inqueue, process and outqueue time. This is an average.

**Average Output Queue Time Per Transaction(µs)**
- Displays the average amount of time transaction output waiting in the message queue before being delivered to its final destination.

**Average Processing Time Per Transaction(µs)**
- Displays the average transaction processing time. This is the amount of time it took to process the transaction once it’s scheduled.

**Transaction Group Name**
- Displays the name of the transaction group.

**Transaction Rate Per Second**
- Displays the transaction rate per second over the requested interval.

**MQ Queue Managers**

CA APM Cross-Enterprise monitors data for the Queue managers configured for your environment. For more information about configuring queue managers, see, [Configure the Cross-Enterprise_APM_Dynamic.properties File](#) (see page 38).

The MQ queue manager metrics appear under the folder: MQ Queue Managers|<queue manager name>.

Additionally, the following queue manager-related data is reported in subfolders:

- [Configuration properties](#) (see page 174)
- [Queues](#) (see page 178)
- [Status (Queue Managers)](#) (see page 175)
These are the MQ queue manager metrics:

**Aggregated Maximum Queue Depth Reached**
- Displays an aggregated value of all the queue managers for the maximum value from all maximum queue depth reached.

**Aggregated Queue Manager Value**
- Displays an aggregated value of all the queue managers for the maximum value from all queue manager values.

**Configuration Properties (Queue Managers)**

Configuration Properties for the queue manager. The values of these do not change frequently.

The MQ queue manager configuration properties metrics appear under the folder: MQ Queue Managers|<queue manager name>|Configuration Properties.

These configuration property metrics are reported for queue managers.

**Channel Initiator Address Space ID**
- Displays the identifier of the channel initiator address space.

**Channel Initiator Job Name**
- Displays the name of the channel initiator job.

**Command Prefix**
- Displays the command prefix.

**DB2 Data Sharing Group Name**
- Displays the name of the DB2 Data Sharing Group.

**DB2 Name**
- Displays the name of the group attach or DB2.

**Monitored by CA SYSVIEW**
- Indicates whether the queue manager is or is not being monitored by CA SYSVIEW.
  - Possible values are:
    - **MON**
      - The queue manager is being monitored by the product.
    - **blank**
      - The queue manager is not being monitored by the product

To have the product monitor a queue manager you must have a MONITOR statement specified in the MQSMON member of PARMLIB to INCLUDE the queue manager either explicitly or through generics.
OTMA XCF Group Member Name Of The IMS Bridge
Displays the OTMA XCF group member name of the IMS Bridge.

OTMA XCF Group Of The IMS Bridge
Displays the OTMA XCF group of the IMS Bridge.

Queue Manager Address Space ID
Displays the address space identifier of the queue manager.

Queue Manager Job Name
Displays the name of the queue manager job.

Queue Manager Name
Displays the name of the queue manager.

Queue Sharing Group Name
Displays the name of the queue sharing group.

Web Sphere MQ Version
Displays the version of the WebSphere MQ.

Status (Queue Managers)
Status metrics for the queue manager. The values of these change frequently.

The MQ queue manager status metrics appear under the folder: MQ Queue Managers\<queue manager name>\Status.

These status metrics are reported for queue managers:

Amount of Real Storage Used (kb)
Displays the amount of real storage in kilobytes the queue manager address space is using in the private region.

CPU Time Accumulated (µs)
Displays the accumulated CPU time in CPU microseconds used by the queue manager address space.

CPU Time Per Interval (µs)
Displays the accumulated CPU time in CPU microseconds used by the job for the interval specified.
Channel Initiator
Displays the channel initiator status. Possible values are:

**ACTIVE**
The channel initiator is active.

**INACTIVE**
The channel initiator is not active.

Executed Amount Of Wall Clock Time (sec)
Displays the amount of time it takes the wall clock to execute for the queue manager address space.

Executed I/O Operations Count
The number of I/O operations performed by the queue manager address space.

Executed I/O Operations Count Per Interval
Displays the number of I/O operations performed by the queue manager address space for the specified interval.

Queue Manager
Displays the queue manager status. Possible values are:

**ACTIVE**
The queue manager is active.

**INACTIVE**
The queue manager is not active.

**QUIESCE**
The queue manager is quiescing.

Queue Manager Value
Displays the status indicator for the Queue Manager Status with these values.

0

NONE

1

NORMAL

2

HIGH
3
WARNING
4
PROBLEM

MQ Alerts

All metrics are reported on every polling interval unless the alert has been acknowledged. In which case the metrics are absent and go gray.

Only the alerts that are unacknowledged appear in the Workstation Investigator tree. If there are no unacknowledged alerts these metrics will be zero.

Unacknowledged Problem Count
The current number of MQ alerts that have a status of problem.

Unacknowledged Alert Count
The current number of unacknowledged MQ alerts.

Unacknowledged Warning Count
The current number of MQ alerts that have a status of warning.

The metrics for each MQ alert appear under the folder structure: MQ Queue Managers|<manager>|Alerts

Alert Status
The current alert threshold status. This value can be NONE, NORMAL, HIGH, WARNING, or PROBLEM.

Alert Status Value
The current alert threshold status as a numeric value. This value can be 0=NONE, 1=NORMAL, 2=HIGH, 3=WARNING, or 4=PROBLEM.

Description
A description of the alert.

Name
The name of the alert. In CA SYSVIEW, it is the variable name for the data collection element of the alert. This metric is the prefix of the alert folder name.

Priority
The priority of the alert from 0 through 999 with 999 having the highest priority.

Queue Manager
The name of the queue manager
Resource Name (Optional)

The resource of the alert. CA SYSVIEW is the resource argument to qualify the collection element of the alert. This metric will not appear if it has no value. This becomes the second underscore separated portion of the alert’s folder name, when it exists.

Rule Type

The exception rule type. Possible values are:

- UPPER indicates the upper limit threshold.
- LOWER indicates the lower limit threshold.
- CHANGE indicates a change in the value threshold.
- STATE indicates a state exception.

Subgroup

The subgroup classification for the alert. Possible values are:

- CHANNEL - MQ channel alert
- PAGESET - MQ page set alert
- POOL - MQ buffer pool alert
- QMGR - MQ queue manager alert
- QUEUE - MQ queue alert

Value

The value last used during threshold processing. If the resource does not currently have an associated threshold definition, the value is the last value the data collector collects.

MQ Queues

CA APM Cross-Enterprise monitors data for the queues that belong to queue managers configured for your environment. For more information about configuring queues, see Configure the Cross-Enterprise_APM_Dynamic.properties File (see page 38).

The MQ queues metrics appear under the folder: MQ Queue Managers|<queue manager name>|Queues.

Additionally, the following queue-related data is reported in subfolders:

- Configuration Properties (Queues) (see page 179)
- Status (Queues) (see page 180)
These are the queues metrics:

**Aggregated Get Messages Value**

Displays the aggregate value of the maximum value from all get messages value metrics for all queues specified in the queue manager.

**Aggregated Put Messages Value**

Displays the aggregate value of the maximum value from all put messages value metrics for all queues specified in the queue manager.

**Maximum Queue Depth (% Queue Full)**

Displays the aggregate value of the maximum value from all current queue depth (% Queue Full) for all queues specified in the queue manager.

**Maximum Queue Depth Reached**

Displays the aggregate value of the maximum value from all maximum queue depth reached for all queues specified in the queue manager.

**Configuration Properties (Queues)**

Configuration Properties for the queues. The values of these do not change frequently. These configuration property metrics are reported for queues that belong to queue managers.

The MQ queue configuration properties metrics appear under the folder: MQ Queue Managers|<queue manager name>| Queues|<queue name>|Configuration Properties.

These are the queues metrics:

**Description**

Displays the description of the queue.

**Get Messages**

Displays Get operations allowed or inhibited with these values.

- Enabled
- Disabled

**Get Messages Value**

Displays the value of the Get Messages command with these values.

- 0
  - Enabled
- 1
  - Disabled
Max Queue Depth

Maximum number of messages allowed on queue.

Put Messages

Displays the Put operations allowed or inhibited with these values.

- Enabled
- Disabled

Put Messages Value

Displays the value of the Put Messages command with these values.

- 0
  - Enabled
- 1
  - Disabled

Queue Name

Displays the name of the queue.

Status (Queues)

Status metrics for the queues. The values of these change frequently.

The MQ queue status metrics appear under the folder: MQ Queue Managers | <queue manager name> Queues | <queue name> | Status.

These status metrics are reported for queues that belong to queue managers.

Current Queue Depth

Displays the number of messages on the queue.

Current Queue Depth Percentage (% Queue Full)

Displays the percentage of fullness of the queue.

Last Elapsed Get Time (ms)

Displays the time elapsed in milliseconds since the last Get command was executed.

Last Elapsed Put Time (ms)

Displays the time elapsed in milliseconds since the last Put command was executed.

Last Get Date

Displays the date of the last Get command.

Last Get Time

Displays the time of the last Get command.
Last Put Date
Displays the date of the last Put command.

Last Put Time
Displays the time of the last Put command.

Oldest Message Age
Controls the collection of the oldest message age metric for MQ queues. Collecting this metric has a performance impact, so it is off by default.

Open Input Count
Displays the number of handles that are currently valid for removing messages from the queue.

Open Output Count
Displays the number of handles that are currently valid for adding messages to the queue.

Queue Time (Long Term Avg.)
Displays the average time, in milliseconds, that a message spent on the queue, based on activity over a longer period. Compare with Queue Time (Short Term Avg).

Queue Time (Short Term Avg.)
Displays the average time, in milliseconds, that a message spent on the queue, based on activity over a shorter period. Compare with Queue Time (Long Term Avg.)

TCP/IP Stacks

Cross-Enterprise APM monitors data for TCP/IP stacks.

The TCP/IP Stacks metrics appear under the folders: TCPIP Stacks|<stack>.

The status for TCP/IP stacks is reported in the status subfolder. For more information about status metrics, see Status (TCP/IP Stacks) (see page 183).

Amount of Real Storage Used (kb)
Displays the amount of real storage in kilobytes the TCP/IP stack address space is using in the private region.

CPU Time Accumulated (µs)
Displays the accumulated CPU time in microseconds, used by the TCP/IP stack.

CPU Time Per Interval (µs)
Displays the CPU time per interval for the TCP/IP stack.
Communications Server Version and Release

Displays the Communications Server version and release in the format v.r. Possible values are:

1.7

Communications Server 1.7

1.6

Communications Server 1.6

1.5

Communications Server 1.5

1.4

Communications Server 1.4

Enabled for IPV6

Indicates whether the TCP/IP is enabled or not for Internet Protocol version 6 (IPv6).

Executed Amount Of Wall Clock Time (sec)

Displays the amount of time it takes the wall clock to execute for the TCP/IP stack address space.

Executed I/O Operations Count

Displays the number of I/O operations performed by the TCP/IP stack address space.

Executed I/O Operations Count Per Interval

The number of I/O operations performed by the TCP/IP stack address space for the specified interval.

Hostname

Displays the host name the TCP/IP stack retrieved at startup from the TCPIP.DATA file that was found.
Monitored By CA SYSVIEW

Indicates whether or not the TCP/IP stack is being monitored by the product with these values.

**MON**

The TCP/IP stack is being monitored by the product.

**blank**

The TCP/IP stack is not being monitored by the product.

To have the product monitor a TCP/IP stack, you must have a `MONITOR` statement specified in the `TCPMON` member of `PARMLIB` to `INCLUDE` the TCP/IP job name either explicitly or through generics.

Status (TCP/IP Stacks)

The TCP/IP stacks status metrics appear under the folder: TCPIP Stacks | <stack> | Status.

These status metrics are reported for TCPIP stacks:

**Address Space**

Displays the status of the TCP/IP address-space with these values.

**ABENDED**

The TCP/IP address space has ended abnormally.

**ACTIVE**

The TCP/IP address space is active.

**STOPPING**

The TCP/IP address space is in the process of stopping.

**STOPPED**

The TCP/IP address space has been stopped.

**DOWN**

The TCP/IP address space is in a DOWN condition.

**Address Space Value**

Displays the status indicator for the address space with these values.

- 0 indicates NONE.
- 1 indicates NORMAL.
- 2 indicates HIGH.
- 3 indicates WARNING.
- 4 indicates PROBLEM.
DB2 z/OS Subsystems Metrics

The Cross-Enterprise APM agent can be configured to collect metrics from one or more DB2 subsystems running on the local LPAR. Each monitored DB2 subsystem will report metrics in the following categories:

- Buffer Pool (see page 184)
- Distributed Activity (see page 185)
- EDM Pool (see page 186)
- Exceptions (see page 187)
- General (see page 188)
- Group Buffer Pool (see page 189)
- Locks (see page 190)
- Log Activity (see page 191)
- Misc (see page 191)
- Subsystem CPU (see page 193)
- Workload (see page 194)

Buffer Pool

These buffer pool metrics are reported for each monitored DB2 subsystem.

Asynchronous Writes
Displays the number of write I/O operations made during the last polling interval.

Available Pages (%)
Displays the percentage of buffer pool pages that are free for use by other applications.

Dataset Opens
Displays the total number of times data sets were physically opened for the buffer pool during the last polling interval.

Page Get Requests
Displays the number of data page access requests made during the last polling interval.

Page Read Efficiency
Displays the percentage of time that the data requested is serviced by data already in the buffer pool and not loaded from disk during the last polling interval.
Page Write Efficiency
Displays the ratio of the number of buffer pool pages that are written to the number of write operations that are performed during the last polling interval.

Page Write Requests
Displays the number of update buffer pool pages that are written out to disk during the last polling interval.

Prefetch Failed
Displays the number of times that DB2 failed to honor a prefetch request because the prefetch threshold was reached during the last polling interval.

Prefetch IO
Displays the number of prefetch read I/O requests made during the last polling interval.

Prefetch Reads
Displays the number of pages that have been read into the buffer pool using sequential prefetch I/O operations during the last polling interval.

Prefetch Requests
Displays the number of requests to pre-read pages for index and table spaces during the last polling interval.

Synchronous IO
Displays the number of synchronous I/O operations that have occurred to or from DB2 pagesets during the last polling interval.

VPool Size
Displays the number of buffers that are allocated for all virtual buffer pools.

Distributed Activity
These distributed SQL activity metrics are reported for each monitored DB2 subsystem.

Rows Received
Displays the number of rows of data retrieved from the remote server location during the last polling interval.

Rows Sent
Displays the number of rows of data sent to the remote requester location during the last polling interval.
**SQL Received**
Displays the number of SQL statements received from the remote requester location during the last polling interval.

**SQL Sent**
Displays the number of SQL statements sent to the remote server during the last polling interval.

**EDM Pool**

These EDM pool metrics are reported for each monitored DB2 subsystem.

**Cursor Table Load (%)**
Displays the ratio of how many load requests resulted in no I/O due to the requested resource already being loaded during the last polling interval.

**DBD Load (%)**
Displays the ratio of how many load requests for DBD (database descriptor) pages resulted in no I/O due to the resource already being loaded during the last polling interval.

**DBD Pool Free Pages**
Displays the number of free pages in the DBD pool free chain.

**DBD Pool Full Failures**
Displays the number of times an application has a DBD loaded into the DBD pool, but was unable to do so because all pages in the DBD pool were in use during the last polling interval.

**DBD Pool Pages**
Displays the number of pages that are allocated to the DBD pool.

**DBD Pool Pages Available (%)**
Displays the percentage of DBD Pool pages that are free for use by other applications.

**DBD Used Pages**
Displays the number of pages of the DBD pool that are allocated to the database descriptors (DBDs).

**Dynamic Statement Load (%)**
Displays the percentage of how many requests for dynamic statements are satisfied using statements already contained within the dynamic statement cache during the last polling interval.
EDM Pool Full Failures
Displays the number of times that DB2 was unable to find or replace pages in the EDM pool because all pages were in use during the last polling interval.

Package Table Load (%)
Displays the ratio of how many load requests for package table pages resulted in no I/O due to the resource already being loaded during the last polling interval.

Skeleton Cursor Table Pages
Displays the number of pages of the EDM pool that are allocated to skeleton cursor tables (SKCTs).

Skeleton Package Table Pages
Displays the number of pages of the EDM (environmental descriptor manager) pool that are allocated to skeleton package tables (SKPTs).

Skeleton Package Table Pages Available (%)
Displays the percentage of skeleton package table pages that are free for use by other applications.

Statement Pool Free Pages
Displays the number of free pages in the EDM statement pool.

Statement Pool Full Failures
Displays the number of EDM statement pool full failures encountered during the last polling interval.

Statement Pool Pages
Displays the total number of pages in the EDM statement pool.

Statement Pool Used Pages
Displays the number of pages used in the statement pool.

Exceptions
These Insight exception metrics are reported for each monitored DB2 subsystem.

Application Critical Exceptions
Displays the number of critical application exceptions detected during the last exception cycle.

Application Warning Exceptions
Displays the number of warning application exceptions detected during the last exception cycle.
Database Critical Exceptions
Displays the number of critical database exceptions detected during the last exception cycle.

Database Warning Exceptions
Displays the number of warning database exceptions detected during the last exception cycle.

Subsystem Critical Exceptions
Displays the number of critical subsystem exceptions detected during the last exception cycle.

Subsystem Warning Exceptions
Displays the number of warning subsystem exceptions detected during the last exception cycle.

Total Critical Exceptions
Displays the total number critical exceptions (subsystem, database, and application) detected during the last exception cycle.

Total Warning Exceptions
Displays the total number of warning exceptions (subsystem, database, and application) detected during the last exception cycle.

General

These general metrics are reported for each monitored DB2 subsystem.

Availability
Displays whether you can connect to the database in text form. This metric can have one of the following values:

AVAILABLE
Displays if the Cross-Enterprise APM Agent can establish a connection to the Insight agent monitoring the selected instance of DB2.

UNAVAILABLE
Displays if the selected DB2 subsystem, Insight agent, or Xnet communication infrastructure is down. This value also displays if the monitored DB2 subsystem was recycled since the last polling interval.
Availability Value
Displays whether you can connect to the database in numeric form. This metric can have one of the following values:

1
Displays if the Cross-Enterprise APM Agent can establish a connection to an Insight agent monitoring the selected instance of DB2.

0
Displays if the selected DB2 subsystem, Insight agent, or Xnet communication infrastructure is down. This value also displays if the monitored DB2 subsystem was recycled since the last polling interval.

DB2 Start Time
Displays the date and time that the subsystem was started.

Data Sharing Group Name
Displays the DB2 data sharing group name (if any).

Data Sharing Member Name
Displays the DB2 member name within a DB2 data sharing group (if any).

Location Name
Displays the location name by which distributed applications connect to the DB2 subsystem.

Release Number
Displays the version number of the monitored DB2 subsystem.

SMF ID
Displays the SMF ID for the z/OS system.

Subsystem Name
Displays the name of the monitored DB2 subsystem.

Group Buffer Pool
These group buffer pool metrics are reported for each monitored DB2 subsystem.

Page Data Reads
Displays the number of pages that are read from the group buffer pool during the last polling interval.

Page Empty Reads
Displays the number of times a read was attempted from the group buffer pool where the requested data was not found in the pool during the last polling interval.
Page Read Efficiency

Displays the ratio of read requests where data was returned to total read requests during the last polling interval. A low hit ratio indicates that the average time that a page resides in the group buffer pool is too short.

Write Failures

Displays the number of coupling facility write requests that could not complete because of a lack of coupling facility storage resources during the last polling interval.

Locks

These locking metrics are reported for each monitored DB2 subsystem.

Deadlocks

Displays the number of times an application was unable to obtain a lock from the Lock Manager (IRLM) during the last polling interval because of a deadlock situation.

Escalations

Displays the number of times that DB2 successfully performed a lock escalation on a table space during the last polling interval.

Global Requests

Displays the global number of lock requests for physical locks (P-locks) during the last polling interval.

Global Suspensions

Displays the number of suspends occurring because of an IRLM global resource contention (IRLM lock states were in conflict) during the last polling interval.

Local Requests

Displays the number of times that DB2 sent a lock request to IRLM on behalf of the application during the last polling interval.

Local Suspensions

Displays the number of times that an application trying to obtain a lock from the lock manager (IRLM) was delayed during the last polling interval. These delays are due to the resource being held by another task with an incompatible lock.

Timeouts

Displays the number of times that an application was unable to obtain a lock from the lock manager (IRLM) due to timeout during the last polling interval.
Log Activity

These logging metrics are reported for each monitored DB2 subsystem.

Active Log Space Available (%)
Displays the percentage of active log space currently available.

Active Reads
Displays the number of DB2 log reads that were satisfied by data already in the active log data sets during the last polling interval.

Archive Reads
Displays the number of DB2 log reads that were satisfied by data in the archive log data sets during the last polling interval.

Checkpoints
Displays the number of checkpoints DB2 has taken during the last polling interval.

Minutes Between Checkpoints
Displays the average number of minutes between checkpoints since DB2 was last started.

Unavailable Buffer Waits
Displays the number of times DB2 places data into a log buffer but no log buffer was available during the last polling interval.

Write Forced
Displays the number of times DB2 issued a synchronous WRITE request to the active log during the last polling interval.

Write No Waits
Displays the number of times DB2 issued a NOWAIT WRITE request to the active log during the last polling interval.

Write Waits
Displays the number of wait log write requests that are encountered during the last polling interval.

Misc

These miscellaneous metrics are reported for each monitored DB2 subsystem.

Current Starjoin Pool Size
Displays the current size of the starjoin pool in MB.

Current Starjoin Pool Used (%)
Displays the percentage of the starjoin pool currently in use.
DDF Status
Indicates whether the Distributed Data Facility (DDF) is started (ACTIVE) or not (INACTIVE).

DDF Status Value
Indicates whether the Distributed Data Facility (DDF) is started (1) or not (0).

Dataset Open (%)
Displays the current number of database data sets open as a percentage of the DSMA MAX DSNZP ARM parameter.

Maximum Starjoin Pool Size
Displays the maximum size of the starjoin pool in MB.

Maximum Starjoin Pool Used (%)
Displays the highest percentage of the starjoin pool that is used since DB2 was last started.

RID Pool Failures
Displays the number of times RID list processing failed due to either the lack of RID storage, the lack of RIDs, or too many concurrent processes during the last polling interval.

RLF Status
Indicates whether the resource limit facility (RLF) is started (ACTIVE) or not (INACTIVE).

RLF Status Value
Indicates whether the resource limit facility (RLF) is started (1) or not (0).

Starjoin Pool Allocation Requests
Displays the number of allocation requests in the starjoin pool that are issued during the last polling interval.

Starjoin Pool Failures
Displays the number of failures that a full starjoin pool causes during the last polling interval.

Workfile Shortage 32K
Displays the number of times that space in a 4-KB tablespace was used because space in a 32-KB tablespace was not available during the last polling interval.

Workfile Shortage 4K
Displays the number of times that space in a 32-KB tablespace was used because space in a 4-KB tablespace was not available during the last polling interval.
Subsystem CPU

These CPU metrics are reported for each monitored DB2 subsystem.

DB2 Elapsed Time
Displays the number of microseconds the DB2 subsystem was active during the last polling interval.

DBM1 CP CPU Usage
Displays the amount of CP CPU used by the DBM1 address space during the last polling interval, which is displayed in microseconds.

DBM1 CPU (%)
Displays the percentage of CPU used by the DBM1 address space during the last polling interval.

DBM1 zIIP CPU Usage
Displays the amount of zIIP CPU used by the DBM1 address space during the last polling interval, which is displayed in microseconds.

DDF CP CPU Usage
Displays the amount of CP CPU used by the DDF address space during the last polling interval, which is displayed in microseconds.

DDF CPU (%)
Displays the percentage of CPU used by the DDF address space during the last polling interval.

DDF zIIP CPU Usage
Displays the amount of zIIP CPU used by the DDF address space during the last polling interval, which is displayed in microseconds.

IRLM CP CPU Usage
Displays the amount of CP CPU used by the IRLM address space during the last polling interval, which is displayed in microseconds.

IRLM CPU (%)
Displays the percentage of CPU used by the IRLM address space during the last polling interval.

IRLM zIIP CPU Usage
Displays the amount of zIIP CPU used by the IRLM address space during the last polling interval, which is displayed in microseconds.

MSTR CP CPU Usage
Displays the amount of CP CPU used by the MSTR address space during the last polling interval, which is displayed in microseconds.
**DB2 z/OS Subsystems Metrics**

**MSTR CPU (%)**
Displays the percentage of CPU used by the MSTR address space during the last polling interval.

**MSTR zIIP CPU Usage**
Displays the amount of zIIP CPU used by the MSTR address space during the last polling interval, which is displayed in microseconds.

**Processor Count**
Displays the number of processors that are currently allocated for the LPAR.

**Total CPU (%)**
Displays the percentage of CPU used by all DB2 address spaces (except for DDF) during the last polling interval.

---

**Workload**

These workload metrics are reported for each monitored DB2 subsystem.

**Aborts**
Displays the number of implicit and explicit ROLLBACKs (ABORTs) processed by the Subsystem Services component of DB2 during the last polling interval.

**Call Requests**
Displays the number of SQL CALL statements that are issued during the last polling interval.

**Create Thread Requests**
Displays the number of successful create thread requests that the DB2 Subsystem Services component processed during the last polling interval.

**Current Background Threads**
Displays the current number of connections to DB2 from batch.

**Current DBAT Threads**
Displays the current number of active remote connections.

**Current Foreground Threads**
Displays the number of TSO connections in use as defined by the IDFORE DSNZPARM parameter.

**Current Threads**
Displays the current number of active users in DB2.
Delete Requests
Displays the number of SQL DELETE statements that are issued during the last polling interval.

Dynamic Requests
Displays the number of SQL DESCRIBE and SQL PREPARE statements that are issued during the last polling interval.

InsUpdDel Requests
Displays the number of SQL INSERT, SQL UPDATE, and SQL DELETE statements that are issued during the last polling interval.

Insert Requests
Displays the number of SQL INSERT statements that are issued during the last polling interval.

Maximum Background Threads
Displays the maximum number of concurrent connections that DB2 allows from batch.

Maximum Batch Users (%)
Displays the percentage of maximum batch connections in use as defined by the IDBACK DSNZPARM parameter.

Maximum DBAT Threads
Displays the maximum number of database access threads (DBATs) that can be allocated concurrently.

Maximum Foreground Threads
Displays the maximum number of users that are allowed to be identified to DB2 from the TSO foreground simultaneously.

Maximum Remote Users (%)
Displays the percentage of maximum remote connections in use as defined by the MAXDBAT DSNZPARM parameter.

Maximum TSO Users (%)
Displays the percentage of maximum TSO connections in use as defined by the IDFORE ZPARM parameter.

Maximum Threads
Displays the maximum number of allied threads (threads that are started at the local subsystem) that can be allocated concurrently.

Maximum Users (%)
Displays the percentage of maximum users currently active in DB2.
Queued Create Thread Requests
Displays the number of create threads the DB2 Subsystem Services component processes that have waited or were queued. This situation is because the maximum number of concurrent threads had been reached during the last polling interval.

SelectOpen Requests
Displays the number of SQL SELECT and SQL OPEN statements that are issued during the last polling interval.

Syncs
Displays the number of successful single phase COMMITs (SYNCs) processed by the Subsystem Services component of DB2 during the last polling interval.

Update Requests
Displays the number of SQL UPDATE statements that are issued during the last polling interval.

CA NetMaster NM for TCP/IP Metric Categories
EPAgent can be configured to collect metrics from one or more CA NetMaster NM for TCP/IP regions. Each monitored region reports metrics in the following categories. To display and familiarize yourself with the metrics, click each category in Workstation Investigator.

LPARs
LPAR01
  DB2 DDF (see page 197)
  EE (see page 198)
  IP Internals (see page 199)
  IP Resources (see page 200)
    CSM (all)
    EE
    ...
  IPSec (see page 200)
  Identification (see page 201)
  Interfaces (see page 202)
    INTRFC01
    INTRFC02
    ...
  Network Activity (see page 203)
  Sockets (see page 204)
    Server
      Port n
      ...

The following fields in the APMEPAGENT parameter group in a region determine the categories of metrics sent:

**IP Server**
Specifies whether metrics for the Sockets category are sent.

**Network Interfaces**
Specifies whether metrics for the Interfaces category are sent.

**Performance Monitoring**
Specifies whether metrics for the IP Resources category are sent.

**Packet Analyzer**
Specifies whether metrics for all other categories are sent.

### DB2 DDF

CA APM Cross-Enterprise monitors data for the following DB2 Distributed Data Facility (DDF) metrics from a connected CA NetMaster NM for TCP/IP region:

**DDF Active Conns**
Displays the current number of active TCP/IP connections to all DDF tasks.

**DDF Active Tasks**
Displays the number of DDF tasks (active job names ending in *DIST) now active on this LPAR.

**DDF Input Bytes/Sec**
Displays the rate of DDF input in bytes per second for all DDF tasks over the last full minute of traffic.

**DDF Output Bytes/Sec**
Displays the rate of DDF output in bytes per second for all DDF tasks over the last full minute of traffic.
For detailed diagnosis of DB2 DDF network activities, use these functions in the CA NetMaster NM for TCP/IP region:

- Use DB2 for z/OS Network Information Center, accessible by the /DB2 panel shortcut.
- Set up DDF-related business applications to join or split the DDF connections by remote addresses, data sharing groups, database applications, and so on.
- Set up packet-based events for the real-time notification of critical DDF connection activities.

**EE**

CA APM Cross-Enterprise monitors data for the following Enterprise Extender (EE) metrics from a connected CA NetMaster NM for TCP/IP region:

**EE Active Conns**
Displays the current number of active EE connections.

**EE BytesRecv (% of stack)**
Displays the number of EE bytes as a percentage of all IP bytes that the EE stack receives.

**EE BytesSent (% of stack)**
Displays the number of EE bytes as a percentage of all IP bytes that the EE stack sends.

**EE RTP LU-LU Sessions**
Displays the current number of active SNA LU-LU sessions that the EE Rapid Transport Protocol (RTP) pipes carry.

**EE RTP Pipes**
Displays the current number of active RTP pipes using EE connections.

**EE RTP Pipes Red (%)**
Displays the percentage of current EE RTP pipes with ARBMODE=RED.

**EE Retransmission (%)**
Displays the percentage of EE IP packets that were retransmitted.

**Note:** The RTP-related metrics measure only the activities that use EE. Some Advanced Peer-to-Peer Networking (APPN) activities do not use EE. To see these non-EE APPN activities on CA Introscope®, monitor and send the APPN Performance Monitoring metrics from the CA NetMaster NM for TCP/IP region.
All these EE metrics come from the latest sample values of EE data sampling. The calculation interval therefore depends on the monitoring interval that is chosen for EE Performance Monitoring.

For detailed diagnosis of EE activities, use Enterprise Extender Management in the CA NetMaster NM for TCP/IP region, accessible by the /EE panel shortcut.

**IP Internals**

CA APM Cross-Enterprise monitors data for the following metrics from a connected CA NetMaster NM for TCP/IP region:

**IP Fragmentation (%)**
Displays the percentage of IP fragmentation.

**IP Reassembly (%)**
Displays the percentage of IP reassemblies.

**TCP Retransmission (%)**
Displays the percentage of TCP retransmissions.

**UDP Discards (%)**
Displays the percentage of UDP discards.

*Note:* These percentage metrics show the latest sample values of the unqualified stack attributes. The value is the maximum of the latest attribute sample values over all monitored stacks (sample must have been within the last hour).

**Stack Names**
Displays the names of all monitored stacks on this LPAR.

These metrics provide a broad indicator that at least one of the monitored stacks on this LPAR has exceeded a stack internal performance threshold recently.

For example, an IP Fragmentation % value of 13 means that one of the IP stacks active on this LPAR had this value the last time IP Fragmentation was sampled.

Identify and examine in detail the individual stack with the high IP Fragmentation % value using the CA NetMaster NM for TCP/IP region. See the Condition Summary, Stack IP, TCP, and UDP Layers section.

To send metrics continually for a specific IP stack, specify the stack name in the Performance Monitoring filter. You specify the filter in the APMEPAGENT parameter group of the region.
IP Resources

CA APM Cross-Enterprise monitors data for IP resource and node metrics from a connected CA NetMaster NM for TCP/IP region. You configure the region to send these metrics (or numeric attributes) through the APMEPAGENT parameter group.

IPSec

CA APM Cross-Enterprise monitors data for the following IPSec metrics from a connected CA NetMaster NM for TCP/IP region:

Dynamic Tunnels
Displays the current number of dynamic tunnels.

IKE Tunnels
Displays the current number of IKE tunnels.

IP Pkts Denied (%)
Displays the percentage of packets that an IP filter denies for any reason.

IP Security Filters
Displays the number of IP filters.

IPSec Traffic Detected?
Displays whether any IPSec traffic has been detected on this LPAR: YES or NO.

For detailed diagnosis of IPSec and SSL/TLS network security, use IP Security in the CA NetMaster NM for TCP/IP region, accessible by the /SECURE panel shortcut.
Identification

CA APM Cross-Enterprise monitors data for the following Identifications metrics from a connected CA NetMaster NM for TCP/IP region:

**IP Host address**
- Displays the IP host address of this LPAR.

**IP Host name**
- Displays the IP host name of this LPAR.

**LPAR**
- Displays the LPAR name (for example, SYSA).

**Operating System**
- Displays the version of the operating system (for example, IBM z/OS 01.12.00).

**Processor**
- Displays the ID of the physical processor (for example, IBM z Series, Physical Processor ID 002817.M32.IBM.02.0000006F686).

**Sender**
- Displays the details of the region sending this metric feed (for example, CA NetMaster, Region NETM44 Domain NM44 Release Level 070300).

**Sender URL**
- Displays the web URL of the region.

If you have the CA NetMaster NM for TCP/IP license, you can access this URL to use the IP Summary and IP Growth Tracker links on the login page. These functions complement the metrics in CA Introscope®, and require no login ID or password to access.

**Sysplex**
- Displays the name of the sysplex (for example, PLEXAA).

To identify an LPAR uniquely in the NetMasterAgent metric tree, its name has the sysplex name as the prefix (for example, PLEXAA-SYSA). The LPAR names are unique within a sysplex, but can be duplicated in other sysplexes.
Interfaces

CA APM Cross-Enterprise monitors data for the following Interfaces metrics from a connected CA NetMaster NM for TCP/IP region:

**Bandwidth**
- Displays the total available bandwidth.

**Note:** This metric is available only for physical interfaces such as OSAs, where the total available bandwidth is known.

**Input Bandwidth Utilization (0.01%)**
- Displays the percentage of available bandwidth for this stack network interface that inbound data uses.

**Output Bandwidth (0.01%)**
- Displays the percentage of available bandwidth for this stack network interface that outbound data uses.

**Packets Discarded (0.01%)**
- Displays the percentage of packets (both sent and received) that were discarded, despite containing no errors.

This interface was unable to process these packets, possibly because of interface buffer space or other resource constraints. Interface capacity shortages or configuration problems can prevent processing.

**Packets in Error (0.01%)**
- Displays the percentage of packets (both sent and received) that contained errors.

Interface hardware or line problems can cause interface packet errors.

All interface metrics are sent every 5 minutes. Values for the loopback and virtual (zero traffic) interfaces are not included.

All these Interface metrics come from the latest sample values of stack network interface data sampling. The calculation interval therefore depends on the monitoring interval that is chosen for stack network interface Performance Monitoring.

For detailed diagnosis of stack network interface activities, use these functions in the CA NetMaster NM for TCP/IP region:
- Use Stack Interface and Device Links, accessible by the /DEVLINK panel shortcut.
- Use the stack network interface performance data displays (WI command next to a stack on the IP Resource Monitor).
Network Activity

CA APM Cross-Enterprise monitors data for the following Network Activity metrics from a connected CA NetMaster NM for TCP/IP region:

TCP Active Conns
Displays the current number of active TCP/IP connections, summed for all monitored stacks.

IP Input Bytes/Sec
Displays the rate of total IP input in bytes per second for all stacks on this LPAR.

IP Output Bytes/Sec
Displays the rate of total IP output in byte per second for all stacks on this LPAR.

Telnet Active Conns
Displays the current number of active Telnet connections.

FTP Active Conns
Displays the current number of active File Transfer Protocol (FTP) transfers.

Sysplex Distributor Current Conns
Displays the number of currently and recently active connections that are redirected by this LPAR.

If there is no TCP/IP stack in this LPAR functioning as a sysplex distributor distributing host, then the value of this metric is always zero.

Redirected connections are counted in this metric feed until they have had no observed packet activity for the age-out period (a few minutes).

For detailed diagnosis of the network connection workload, use these functions in the CA NetMaster NM for TCP/IP region:

- Use STACK workload monitoring to alert on workload attributes.
- Use the TCP Applications activity display (accessible by the /ASMON.TC panel path) to compare how different tasks are contributing to network activity.
- Use connection lists to examine where the connections to an individual task are coming from.
Sockets

CA APM Cross-Enterprise monitors data for the following Sockets metrics from a connected CA NetMaster NM for TCP/IP region:

Active Conns
Displays the current number of active connections to this TCP server port, summed for all monitored stacks.

Input Bytes/Sec
Displays the rate of input to this TCP server port in bytes per second over the last full minute.

Output Bytes/Sec
Displays the rate of output from this TCP server port in bytes per second over the last full minute.

Backlog Q Depth
Displays the current number of requests in the TCP backlog queue.

Avg Appl Response (10 ms)
Displays the time between the following events:

■ When the local application replied with the first ACK to a received request
■ When the local application then sends the next data packet to respond to the request

An average of its local application response time is maintained for each TCP connection. Then the average of these values is taken for all concurrently active TCP connections with this port that have had packet activity within the last few minutes. This value is recalculated every 5 minutes.

Note: This metric is most meaningful with TCP applications that communicate in a regular request-response pattern, such as HTTP.

The measurement unit is 10 ms (1/100th second), that is, \(234 = 2.34\) seconds.

Time to 1st Response (10 ms)
Displays the time between the following events:

■ When the local application replied with the first ACK to a received request
■ When the local application then sends the next data packet to respond to the request

This metric is equivalent to the time to first response metrics other CA APM products provide.
The local average application response time is continually measured and averaged for every turn in the TCP connection. In contrast, the time to first response is only measured once per TCP connection. The average of these values is then taken for all concurrently active TCP connections with this port that have had packet activity within the last few minutes. This value is recalculated every 5 minutes.

**Note:** This metric is most meaningful with TCP applications that communicate in a regular request-response pattern, such as HTTP.

The measurement unit is 10 ms (1/100th second), that is, 234 = 2.34 seconds.

For detailed diagnosis of TCP server port activities, use these functions in the CA NetMaster NM for TCP/IP region:

- Use ASMON monitoring to alert on port attributes.
- Set up business applications to split connections to this port by remote addresses or to combine this port traffic with related ports.
- Set up packet-based events for real-time notification of critical TCP port connection, workload, fragmentation, and error activities.
- Use SmartTrace to for real-time packet stream viewing and deep packet inspection of the traffic flowing over a specific connection with a port.
- Use multiple TCP tracing in SmartTrace to trace different connections with a port separately.

**Top Lists**

CA APM Cross-Enterprise monitors data for the following Top Lists, \( n \) metrics from a connected CA NetMaster NM for TCP/IP region. \( n \) is 01 through 10.

**App by Bytes name**

Displays the name of the \( n \)th highest TCP application (address space) when sorted by byte throughput.

**App by Bytes value**

Displays the total (input and output) byte throughput for the \( n \)th application during the last full five clock minutes.

**App by Conns name**

Displays the name of the \( n \)th highest TCP application (address space) when sorted by active connections.

**App by Conns value**

Displays the number of concurrent active TCP/IP connections with the \( n \)th application, as at the sample time.
Port by Bytes name
Displays the name of the $n$th highest TCP server port when sorted by byte throughput.

Port by Bytes value
Displays the total (input and output) byte throughput for the $n$th TCP server port during the last full five clock minutes.

Port by Conns name
Displays the name of the $n$th highest TCP server port when sorted by active connections.

Port by Conns value
Displays the number of concurrent active TCP/IP connections with the $n$th TCP server port, as at the sample time.

The following metrics are available for $n=01$ through $05$:

DDF by Bytes name
Displays the name of the $n$th highest DB2 DDF task when sorted by byte throughput.

DDF by Bytes value
Displays the total (input and output) byte throughput for the $n$th DB2 DDF task during the last full five clock minutes.

DDF by Conns name
Displays the name of the $n$th highest DB2 DDF task when sorted by active connections.

DDF by Conns value
Displays the number of concurrent active TCP/IP connections with the $N$th DB2 DDF task, as at the sample time.

For more displays of the network top users, use these functions in the CA NetMaster NM for TCP/IP region:
- Use IP network Summary Display, accessible by the /IPSUM panel shortcut.
- Use IP Growth Tracker, accessible by the .IPGT panel shortcut.
Chapter 6: CA NetMaster NM for TCP/IP Reports

CA NetMaster NM for TCP/IP integration provides the following report templates:

- NetMaster Enterprise Extender Capacity Planning
- NetMaster Network Capacity Planning
- NetMaster Network Interface Performance
- NetMaster Server Port Performance

These templates work with the default metrics without modification. You can use these report templates as a basis for constructing other templates.

Note: For information about how to work with report templates, see the CA Application Performance Management Workstation User Guide.

Report Templates

CA NetMaster NM for TCP/IP integration provides the following report templates:

- NetMaster Enterprise Extender Capacity Planning
- NetMaster Network Capacity Planning
- NetMaster Network Interface Performance
- NetMaster Server Port Performance

These templates work with the default metrics without modification. You can use these report templates as a basis for constructing other templates.

Note: For information about how to work with report templates, see the CA Application Performance Management Workstation User Guide.
Appendix A: Troubleshoot CA APM Cross-Enterprise

This section contains the following topics:

- Problems with the SMF Socket Connection (see page 209)
- Some Transactions Do Not Appear in the Transaction Trace Viewer (see page 210)
- SMF Transactions Traces Missing (see page 211)
- Correlation ID NotFound (see page 212)
- No Data in a CA NetMaster NM for TCP/IP Metric Category (see page 213)

Problems with the SMF Socket Connection

**Symptom:**

The CA APM Cross-Enterprise stops immediately after startup.

This problem occurs when the port specified in the `ppz.smf.socket.port` property of the `Introscope_Cross-Enterprise_APM.profile` file is in use.

The CA APM Cross-Enterprise log file shows the following error message:

```
[ERROR]
   [com.wily.powerpack.sysview.multithread.SMFReaderMasterThread] Socket_Open:
   Error creating server socket: java.net.BindException: EDC8115I Address already in use.

[ERROR]
   [com.wily.powerpack.sysview.multithread.SMFReaderMasterThread] Socket_Open:
   Error probably caused by another copy listening on same port. Exiting
```

**Solution:**

Reserve the port in `ppz.smf.socket.port` property for the WILYZOS job.

This port is required for CA SYSVIEW to submit the SMF transaction records to the CA APM Cross-Enterprise. If you do not reserve this port, you do not get any SMF records from CA SYSVIEW. You also do not get any CICS back-end transaction traces from CA APM Cross-Enterprise.
Some Transactions Do Not Appear in the Transaction Trace Viewer

**Symptom:**

Some front-end or back-end transactions do not appear in the Transaction Trace viewer.

**Solution:**

The following reasons can cause transactions not to appear:

- The transaction trace have been created to include or exclude back-end transactions.
- A transaction trace have been created, and the Trace All Supported Agents option was not selected.
- The Trace selected Agents option and CA APM Cross-Enterprise were not selected for back-end transactions.
- The front-end agent has not been selected for front-end transactions.
- The transaction trace have been created with inapplicable criteria selected.

Solutions follow:

- Verify that you have selected the appropriate criteria.
  
  **Note:** For more information about how to create a transaction trace to include front-end or back-end transactions, see About Cross-Process Transaction Traces.

- To determine if the criteria selection is the problem, clear all transaction trace options except for the User ID does not exist option. Selecting this option allows all traces to be delivered to the transaction trace session window. This test confirms if a filter-specific issue exists.
Transactions do not appear in the Transaction Trace Viewer:

- If front-end transactions are not appearing in the Transaction Trace Viewer, verify that the transactions that invoke web services, CTG, or MQ traces are running.
  
  You can verify the web service, CTG CA SYSVIEW tracer, or WebSphere MQ live metric data for respective front-end agents in the Investigator tree.
  
  - For the CTG CA SYSVIEW tracer, you can see the metrics under the CTGTracer node.
  
  - For the web services tracer, you can see metrics under the WebServices node.
  
  - For the MQ tracer, you can see metrics under the WebSphereMQ node.

- If front-end and back-end traces are not correlated, the back-end trace corresponding to the selected front-end trace has probably not arrived yet. After a short delay, refresh the display by reselecting the trace. If it still is not correlating, the following issues are possible:
  
  - The antiflood threshold is not set to low value. Antiflood threshold limits the number of transactions that are sent to the Enterprise Manager. The recommended default antiflood threshold value is 200 transaction traces per 15 seconds. If you set a low value for the antiflood threshold, many traces are discarded before they are sent to the Enterprise Manager. The likelihood of correlation decreases.
  
  - If the volume of transactions is large, you can start a new transaction trace window with a smaller duration or proper back-end filter setting. This specification increases the chance of retention of the transaction of interest.

**SMF Transactions Traces Missing**

**Symptom:**

The SMF transactions are missing in the Transaction Trace Viewer.

**Solution:**

Ensure that values are the same:

- CA APM Cross-Enterprise SMF record port configuration (`ppz.smf.socket.port`)
- Port that is specified in the group pointed to by the `Wily-Introscope-PortList` parameter for each CICS logger in CA SYSVIEW

To verify that the SMF record for a transaction contains the correlation ID, execute the CA SYSVIEW `CTRANLOG` command. Select an SMF record that was run as the result of some front-end application.
Correlation ID NotFound

**Symptom:**

The Correlation ID was not found in the SMF record.

**Solution:**

CA SYSVIEW have not been able to find the decoration. For more information about how this decoration is done, see About Cross-Process Transaction Traces (see page 98).

**Note:** A decoration is the transaction attribute annotation.

When CA SYSVIEW finds a decorated transaction, it takes the following actions:

1. Create a Correlation IDs segment in the SMF record for the transaction.
2. Write the SMF record to the CA APM Cross-Enterprise TCP/IP port.

To verify that the SMF record for a transaction contains the correlation ID, execute the CA SYSVIEW CTRANLOG command. Select an SMF record that was run as the result of some front-end application. Ensure that the SMF report contains a Correlation IDs segment. If this segment is not in the SMF record, CA SYSVIEW did not find it in the transaction and the record was not sent to the agent.

Possible reasons why SMF records are not given with a correction ID:

- The front-end web services, CTG, and MQ traces are not properly configured. Check the agent log for errors that are related to respective front-end traces and correct them.

- If the front-end traces are configured properly, then it could be a CA SYSVIEW specific issue. Contact your CA SYSVIEW administrator if so.
No Data in a CA NetMaster NM for TCP/IP Metric Category

Symptom:
I cannot see data in a metric category.

Solution:
Sometimes this condition is *not* an error.

Verify that you can see the metric values in the CA NetMaster NM for TCP/IP region. You cannot see Socket, Interface, or IP Resource metric values can be because of the following reasons:

- You did not ask for them to be sent.
- You have not set up some underlying Performance Monitoring.

LPARs that do not have EE or IPSec implemented on them do not show these metric values.
Appendix B: MVS Messages

This section details the messages sent to the MVS message console.

**WILY001I**

CA APM Cross-Enterprise has been started.

**Reason:**
CA APM Cross-Enterprise was started.

**Action:**
No action is required. This message is informational.

**WILY002I**

CA APM Cross-Enterprise is being initialized.

**Reason:**
CA APM Cross-Enterprise is initializing.

**Action:**
No action is required. This message is informational.

**WILY003I**

CA APM Cross-Enterprise has been stopped.

**Reason:**
CA APM Cross-Enterprise was stopped.

**Action:**
No action is required. This message is informational.
WILY004E

Failure to accept the end user license agreement is preventing the agent from starting.

Reason:
CA Cross Enterprise Application Performance Management has an End User License Agreement (EULA) that must be accepted in order to run the product.

Action:
Read the EULA located in the data/EULA.txt file. Setting the following configuration property to "yes" to enable the product indicates that you have read, understood, and will comply with all of the terms and conditions of the EULA:


This property is in the config/Cross-Enterprise_APM_Dynamic.properties file

WILY005E

The metric polling thread failed to initialize.

Reason:
A misconfiguration or fatal error prevented the metric polling thread from initializing.

Action:
Check your settings in Cross-Enterprise_APM_Dynamic.properties, the Cross-Enterprise_APM.log, or the JZOS console for more information about the error.

See the logs for additional messages which will identify the reason the polling thread failed to initialize

WILY006E

CA APM Cross-Enterprise failed to establish a connection to the Enterprise Manager.

Reason:
A misconfiguration or fatal error prevented the CA APM Cross-Enterprise Agent from connecting to the APM Enterprise Manager.

Action:
Check your settings in Intrsoscope_Cross-Enterprise_APM.profile, and the Cross-Enterprise_APM.log for more information about the error.

See the logs for additional messages which will identify the reason it failed to connect.
WILY007E

The SMF record processor failed to initialize.

Reason:
A misconfiguration or fatal error prevented the Cross-Enterprise APM Agent from starting an internal thread which processes the SMF records delivered by CA SYSVIEW and turned into transaction traces.

Action:
Check your settings in Introscope_Cross-Enterprise_APM.profile, the Cross-Enterprise_APM.log, or the JZOS console for more information about the error. See the logs for additional messages which will identify the reason it failed to initialize.

WILY008E

Cross-Enterprise APM initialization failed on the Insight Metric Polling Thread.

Reason:
A misconfiguration or fatal error prevented the Cross-Enterprise APM Agent from starting thread for polling metrics from CA Insight DPM for DB2 for z/OS.

Action:
Check your settings in Introscope_Cross-Enterprise_APM.profile or the Cross-Enterprise_APM.log for more information about the error. See the logs for additional messages which will identify the reason metric polling failed to initialize.

WILY009E

Cross-Enterprise APM Insight Metrics Polling unable to proceed until connection options are changed.

Reason:
A misconfiguration prevented the Cross-Enterprise APM Agent connecting to Xnetmanager to poll metrics from CA Insight DPM for DB2 for z/OS.

Action:
See the Cross-Enterprise_APM.log for additional messages which will identify the reason metric polling stopped and correct the appropriate configuration options in Introscope_Cross-Enterprise_APM.profile. After the configuration is corrected the metric polling will resume automatically.
WILY010E

Cross-Enterprise APM Insight Metrics Polling unable to proceed and will now terminate.

Reason:
A fatal error prevented the Cross-Enterprise APM Agent from polling metrics from CA Insight DPM for DB2 for z/OS.

Action:
Check Cross-Enterprise_APM.log, or the JZOS console for more information about the error and contact technical support if required.