IBM Tools Base for z/OS
Version 1 Release 6

Distributed Access Infrastructure
User's Guide and Reference

IBM
# Contents

About this information ........................................ v

Chapter 1. Distributed Access Infrastructure overview ........................................ 1
  What's new in Distributed Access Infrastructure ........................................ 2
  Distributed Access Infrastructure features ........................................ 3
  Hardware and software prerequisites ........................................ 4
  Distributed Access Infrastructure components ........................................ 5
  Distributed Access Infrastructure architecture ........................................ 6
  Service updates and support information ........................................ 8
  Product documentation and updates ........................................ 9
  Accessibility features ........................................ 11

Chapter 2. Configuring Distributed Access Infrastructure ........................................ 13

Chapter 3. Distributed Access Infrastructure security ........................................ 15
  TCP Server security ........................................ 16
  TAS and SOT security ........................................ 17
  Transport Layer Security and Secure Socket Layer connections ........................................ 18

Chapter 4. Starting Distributed Access Infrastructure ........................................ 19
  Verifying startup ........................................ 20
  Installation verification program ........................................ 21

Chapter 5. Stopping Distributed Access Infrastructure ........................................ 23

Chapter 6. Event logging ........................................ 25
  Enabling event logging ........................................ 26
  Log record structure ........................................ 27
  Sample logs ........................................ 28

Chapter 7. Troubleshooting ........................................ 31
  Runtime error messages (AII) ........................................ 32
  Abend codes ........................................ 44
  Gathering diagnostic information ........................................ 47

Notices ........................................ 49

Index ........................................ 53
About this information

IBM® Tools Base Distributed Access Infrastructure for z/OS® (also referred to as Distributed Access Infrastructure) is an IMS™ Tools product that provides remote access to IMS Tools.

These topics provide instructions for installing, configuring, and using Distributed Access Infrastructure.

To use these instructions, you must have already installed Distributed Access Infrastructure by completing the instructions in the Program Directory for IBM Tools Base for z/OS (GI10-8819), which is included with the product media and is also available on the IMS Tools Product Documentation page.

These topics are designed to help database administrators, system programmers, application programmers, and system operators perform the following tasks:

- Understand the capabilities of the functions that are associated with Distributed Access Infrastructure
- Install and operate Distributed Access Infrastructure
- Customize your Distributed Access Infrastructure environment
- Diagnose and recover from Distributed Access Infrastructure problems
- Use Distributed Access Infrastructure with other IMS products

To use these topics, you should have a working knowledge of:

- The z/OS operating system
- ISPF
- SMP/E
- IMS

Always check the IMS Tools Product Documentation page for the most current version of this information:

Chapter 1. Distributed Access Infrastructure overview

IBM Tools Base Distributed Access Infrastructure for z/OS (also referred to as Distributed Access Infrastructure) enables authorized access to configured IMS Tools from authenticated TCP/IP clients.

Distributed Access Infrastructure acts as a gateway for communication between distributed platforms and z/OS and is delivered as a component of the Tools Base.

Distributed Access Infrastructure is a set of software components that enable distributed clients access to IMS Tools through standard TCP/IP socket communication. Distributed Access Infrastructure acts as a key component in extending the availability of IMS Tools to workstation and browser-based interfaces.

Remote clients must first establish an authenticated connection to the Distributed Access Infrastructure by passing a user ID and password. After authentication, the client program is able to send and receive messages to and from the IMS Tools that the clients are authorized to access.

Topics:
- “What's new in Distributed Access Infrastructure” on page 2
- “Distributed Access Infrastructure features” on page 3
- “Hardware and software prerequisites” on page 4
- “Distributed Access Infrastructure components” on page 5
- “Distributed Access Infrastructure architecture” on page 6
- “Service updates and support information” on page 8
- “Product documentation and updates” on page 9
- “Accessibility features” on page 11
What's new in Distributed Access Infrastructure

This topic summarizes the technical changes for this edition.

New and changed information is indicated by a vertical bar (|) to the left of a change. Editorial changes that have no technical significance are not noted.

October 2016
• Refreshed for Tools Base V1.6
Distributed Access Infrastructure features

Distributed Access Infrastructure includes features that provide many different types of functionality.

Distributed Access Infrastructure offers the following major features:

• Remote connectivity to z/OS hosted tools
• Standard SAF (RACF®) authentication and authorization for tool access
• TCP Secure Socket Layer (SSL) support
• Multi-user TCP/IP access to IMS Tools
• Logging to generate audit trails
Hardware and software prerequisites

Before you install and configure Distributed Access Infrastructure, make sure that your environment meets the minimum hardware and software requirements.

**Hardware prerequisites**

Distributed Access Infrastructure V1.6 operates on any z/OS hardware environment that supports the required software.

**Software prerequisites**

Distributed Access Infrastructure V1.6 is designed to run with IMS V12.1, IMS V13.1, and IMS V14.1.
Distributed Access Infrastructure components


TCP Server

The TCP Server runs in its own z/OS address space that listens for client connections on a user-defined TCP/IP port. When a client connects, the client must first pass security system authentication with a valid user ID and password. If the authentication is successful, the TCP Server acts as a gateway that passes incoming and outgoing messages between the client and a TAS.

Tools Access Server

The Tools Access Server (TAS) runs in its own z/OS address space that is responsible for routing messages to and from tools that are enabled for distributed access. The TAS is responsible for reading incoming messages and routing the messages to the correct IMS Tool.

Subordinate Tools Access Server

The Subordinate Tools Access Servers (SOT) are separate address spaces. SOTs provide an environment for hosting tools whose execution was requested by a client.

Enabled tools for Distributed Access Infrastructure

Distributed Access Infrastructure facilitates the communication to enabled IMS Tools.

All Distributed Access Infrastructure enabled tools use the security credentials of the client to access IMS Tools. Therefore, normal authorization and control of authorization apply for all client access to IMS Tools.

To check if a specific IMS Tool supports distributed access through Distributed Access Infrastructure, see the documentation for that IMS Tool.
Distributed Access Infrastructure architecture

Distributed Access Infrastructure operates in a z/OS environment and uses a TCP Server, the Tools Access Server (TAS), and the Subordinate TAS (SOT) to provide distributed access to IMS Tools products from remote systems.

The following figure illustrates the overall flow of communication from the distributed systems to the IMS Tools products.

Clients that are running on distributed systems first connect to the TCP Server. After clients have successfully authenticated with the TCP Server, client requests are forwarded by the TCP Server to the TAS for routing. TAS selects an SOT to run...
the requested tool and forwards the message to that SOT. Message responses are returned from the SOT to the TCP Server without passing through the TAS, and then back to the client.
Service updates and support information

Service updates and support information for this product, including software fix packs, PTFs, frequently asked questions (FAQs), technical notes, troubleshooting information, and downloads, are available from the web.

To find service updates and support information, see the following website:

Product documentation and updates

IMS Tools information is available at multiple places on the web. You can receive updates to IMS Tools information automatically by registering with the IBM My Notifications service.

Information on the web

The IMS Tools Product Documentation web page provides current product documentation that you can view, print, and download. To locate publications with the most up-to-date information, refer to the following web page:


You can also access documentation for many IMS Tools from the IBM Knowledge Center:

https://www-01.ibm.com/support/knowledgecenter/

IBM Redbooks® publications that cover IMS Tools are available from the following web page:

http://www.redbooks.ibm.com

The Data Management Tools Solutions website shows how IBM solutions can help IT organizations maximize their investment in IMS databases while staying ahead of today’s top data management challenges:


Receiving documentation updates automatically

To automatically receive emails that notify you when new technote documents are released, when existing product documentation is updated, and when new product documentation is available, you can register with the IBM My Notifications service. You can customize the service so that you receive information about only those IBM products that you specify.

To register with the My Notifications service:
1. Go to http://www.ibm.com/support/mysupport
2. Enter your IBM ID and password, or create one by clicking register now.
3. When the My Notifications page is displayed, click Subscribe to select those products that you want to receive information updates about. The IMS Tools option is located under Software > Information Management.
4. Click Continue to specify the types of updates that you want to receive.
5. Click Submit to save your profile.

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. If you have any comments about this book or any other IBM product documentation, use one of the following options:

• Use the online reader comment form, which is located at http://www.ibm.com/software/data/rcf/
* Send your comments by email to comments@us.ibm.com. Include the name of the book, the part number of the book, the version of the product that you are using, and, if applicable, the specific location of the text you are commenting on, for example, a page number or table number.
Accessibility features

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use a software product successfully.

The major accessibility features in this product enable users to perform the following activities:

- Use assistive technologies such as screen readers and screen magnifier software. Consult the assistive technology documentation for specific information when using it to access z/OS interfaces.
- Customize display attributes such as color, contrast, and font size.
- Operate specific or equivalent features by using only the keyboard. Refer to the following publications for information about accessing ISPF interfaces:
  - z/OS ISPF User’s Guide, Volume 1
  - z/OS TSO/E Primer
  - z/OS TSO/E User’s Guide

These guides describe how to use the ISPF interface, including the use of keyboard shortcuts or function keys (PF keys), include the default settings for the PF keys, and explain how to modify their functions.
Chapter 2. Configuring Distributed Access Infrastructure

Information about configuring Distributed Access Infrastructure and other Tools Base components for IMS is provided in IBM Tools Base for z/OS Configuration for IMS.

You can also download a PDF version of this information from the IMS Tools Product Documentation page.
Chapter 3. Distributed Access Infrastructure security

Distributed Access Infrastructure includes various security mechanisms to implement a security policy for checking messages that are passed to and from clients and the IMS Tools.

You can use your SAF compliant security system, such as RACF, with TLS/SSL configured connections to ensure that only trusted and authorized messages are passed.

The system administrator retains full control through the TCP Server and TAS security parameters over login authorizations.

All IMS Tools that are enabled for Distributed Access Infrastructure are authenticated by using the credentials of the client. Therefore, normal authorization and authorization control still apply for all client access to IMS Tools.

Topics:

• “TCP Server security” on page 16
• “TAS and SOT security” on page 17
• “Transport Layer Security and Secure Socket Layer connections” on page 18
TCP Server security

The TCP Server authenticates a user by verifying the user ID and password on the z/OS system where the TCP Server is running. Depending on how you want to manage access, you can optionally base this authentication on security group membership, access to an application security profile, or both.

The TCP Server authenticates users when a connection is established and a logon request is received.

The user ID and password of the client must be defined to the security system on the z/OS system where the TCP Server is running.

Methods for controlling access to the TCP Server

You can manage two types of security schemes to control client access to the TCP Server: group based and application class based.

Group-based security
You can specify the SecurityGroup parameter if you want the TCP Server to limit access by user ID membership in the specified security group. When you specify the SecurityGroup parameter, users must be a member of the specified security group to be successfully authenticated by the TCP Server. If the SecurityGroup value is NONE or is not specified in the configuration file of the server and defaults to NONE, a group name is not used when user IDs are authenticated.

Application class-based security
You can specify the SecurityAppl parameter if you want to use an APPL class resource-based security scheme. By specifying the SecurityAppl parameter, only users that have READ access to that application profile can access the TCP Server. If the SecurityAppl value is NONE or the application name is not defined as an APPL class profile and defaults to NONE, APPL class checking is not performed.

You can specify any combination of these parameters in the TCP Server PROCLIB configuration member.

If neither parameter is specified, any valid user ID and password passes authentication.
TAS and SOT security

TAS and SOT servers do not require security definitions for their own processing. However, you can manage the security for tools hosted by the TAS and SOT.

TAS and SOT security for hosted tools

When a message is sent to TAS and SOT to request the execution of a tool, the security authorities of the client user ID are used when the tool is executed. For example, if a tool accesses a z/OS data set, the security authorities of the client user ID are used to access that data set.

The TCP Server communicates security information to the TAS, and TAS propagates this information to the SOT, which means that TAS and SOT do not require an explicit logon for the client. The user ID that is used by the client to log on to the TCP Server must also be a valid user ID on the z/OS system where the TAS is running.

In the TAS configuration file, you can specify the SecurityAppl configuration parameter so that you can use an APPL class resource-based security scheme for hosted tools. When you specify the SecurityAppl parameter, only users who have READ access to the specified application profile can access the tools. If the SecurityAppl value is NONE or if the application name is not defined as an APPL class profile, APPL class checking does not affect processing in the tool.

Important: The TCP Server and the TAS and SOT do not share SecurityAppl parameter values. The Distributed Access Infrastructure administrator is responsible for ensuring that this parameter is set properly in the configuration files for each server.
Transport Layer Security and Secure Socket Layer connections

Distributed Access Infrastructure allows data to be passed to and from distributed clients and IMS Tools that are enabled for distributed access. Transport Layer Security (TLS) and Secure Socket Layer Security (SSL) can provide security for communication between the IMS Tools that are being accessed and the distributed client.

**Important:** To protect the privacy and integrity of all sensitive data that is being passed through a network, enable TLS/SSL on all sockets that might contain sensitive data.

To enable the TLS or SSL secure communication, you or a network administrator can use the IBM Configuration Assistant for z/OS Communications Server, which is included with z/OS V1.7 or later. IBM Configuration Assistant for z/OS Communications Server is a stand-alone application that provides a graphical user interface (GUI) for configuration. You can use this application to quickly configure TLS policies independent of the configuration and operation of the Distributed Access Infrastructure TCP Server.

For more information about IBM Configuration Assistant for z/OS Communications Server, see the Communications Server IP Configuration Guide that pertains to your current version of z/OS and TCP/IP.
Chapter 4. Starting Distributed Access Infrastructure

To start the Distributed Access Infrastructure, run the TCP Server and the Tools Access Server (TAS).

**Before you begin**

Before starting the TCP and TAS servers, ensure that you have configured the startup parameters and modified the execution JCL for each server.

**Requirement:** Ensure that the XcfGroupName parameter in the TCP Server and TAS configuration files is set to or defaulted to the same value. If the parameter is not set to the same value, the servers cannot communicate with each other.

**About this task**

The Distributed Access Infrastructure servers can run as started tasks, started jobs, or batch jobs. You can choose the method that best fits your installation operations.

After you start the Distributed Access Infrastructure servers, Distributed Access Infrastructure runs continuously in the background, but consumes few resources.

**Procedure**

Start the TCP Server and the TAS.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You want to start the servers as batch jobs.</td>
<td>Add the proper JOB statements in the execution JCL for the TCP Server and the TAS, then submit the job.</td>
</tr>
<tr>
<td>You want to start the servers as started jobs or started tasks.</td>
<td>Execute the z/OS START command: $ server_name</td>
</tr>
</tbody>
</table>

TAS uses the Address Space Create service (ASCRE) to start the SOT address spaces. Based on the number of client requests, TAS can start additional SOT address spaces. As work in SOTs quiesces, TAS terminates unused SOT address spaces. When TAS is stopped, all active SOTs are shutdown. A z/OS operator must not issue a START for the SOT procedure. The SOTs do not respond to a STOP command, but you can cancel an SOT if a problem is detected. If you cancel an SOT while it is actively exchanging messages with a client, the client's session might hang.

**What to do next**

After you start Distributed Access Infrastructure, verify the startup by viewing the AILOG.
Verifying startup

You can verify the Distributed Access Infrastructure startup by viewing messages in AIILOG. These messages show startup information, configuration parameters, and initialization status.

Procedure

1. View the AIILOG for the TCP Server and TAS.
2. Verify that the TCP Server, TAS, and each SOT include an XCF JOIN message, as shown in the following example:

   2009/12/14 11:49:21.53 TAS#####EC05003E 00 STARTUP XCF JOIN Group=DAIGROUP Member=TAS#####EC05003E RC=00000000

   After the XCF JOIN message is displayed in the AIILOG of a server, the server is ready to send and receive messages among z/OS Distributed Access Infrastructure components.

   If the return code of the JOIN is non zero, a reason code is also displayed in the log message. If the server is the first member to join the XCF group, the return and reason codes have a value of 4.

3. Verify that the TCP Server log indicates that the TCP/IP communications have started and that the server is ready to send and receive messages with TCP/IP clients, as shown in the following example:

   2009/12/14 11:50:32.44 NTWKTCPSC753002A 00 STARTUP TCP communication starting, Port: 5124, Max connections: 10

4. Verify that the TCP Server and TAS also issue the following WTO message, which is displayed in the server job log:

   AII0005I Server task initialization has completed

   This WTO message indicates that the internal processes of the server are initialized and are ready to process Distributed Access Infrastructure messages.

   The WTO message is issued before XCF and TCP/IP communication are established.

Results

Verification is complete. If you received any error messages, resolve the errors then restart the startup process.
Installation verification program

The installation and verification program (IVP) verifies the successful installation and configuration of Distributed Access Infrastructure by sending and receiving a message to and from the TCP Server and Tools Access Server.

**Before you begin**

- Successfully start Distributed Access Infrastructure.
- Obtain the following information, which you will need to complete the IVP:
  - The TCP/IP dotted address or domain name of the z/OS system that the TCP server is running on. If you are starting this IVP on the same z/OS system that the TCP server is running on, you can use localhost as domain name.
  - The TCP server listening port number.
  - A TSO ID and password that is valid on the z/OS system that the TCP server is running on.

**Procedure**

1. Open an ISPF application dialog.
2. Issue the following TSO EXEC command in option 6 of the ISPF panel:
   ```
   ex 'high_level_qualifier(aiiivp)'
   ```
   The IVP starts. Messages that describe the IVP process and its prerequisites are displayed.
3. Follow the instructions that are presented by the IVP.
   The IVP issues a message that indicates whether the IVP completed successfully.
   If the IVP was unsuccessful, view the error message in the log file that you created with the IVP.
Chapter 5. Stopping Distributed Access Infrastructure

You can stop Distributed Access Infrastructure to administer maintenance, to change server parameters, or to stop TCP/IP client access to IMS Tools.

Before you begin

When you stop Distributed Access Infrastructure, all TCP/IP client connections are terminated. You might want to check for connected users by viewing the AIILOG and notify them that the system is being stopped.

About this task

Stop the TCP server first to prevent any new connections, and then stop the Tools Access Server (TAS).

Procedure

1. Stop the TCP Server by issuing a STOP command, as shown in the following example:
   
   P TCP_Server_name
   
   The TCP Server accepts the STOP command and completes the following processes:
   • Shuts down all open TCP connections
   • Exits the Distributed Access Infrastructure XCF group
   • Terminates all BPE tasks
   • Terminates the z/OS job

2. Stop the TAS by issuing a STOP command, as shown in the following example:
   
   P TAS_Server_name
   
   The TAS accepts the STOP command and completes the following processes:
   • TAS terminates all active SOTs.
   • Exits the TAS XCF Group.
   
   SOT address spaces are started and stopped by TAS and do not respond to a STOP command. You can cancel an SOT if a problem is detected. If you cancel an SOT while it is actively exchanging messages with a client, the client’s session might hang.

Results

After you have issued the STOP commands, Distributed Access Infrastructure is successfully shut down.
Chapter 6. Event logging

IMS Distributed Access Infrastructure logging can log events that can help you track the status of your system, audit your system, or troubleshoot system errors.

Events, such as login and tool requests, are logged, which creates an audit trail of distributed access and events. The logging functions that are described in these topics pertain to both the TCP Server and TAS.

All Distributed Access Infrastructure Servers write log records to the file that is allocated to ddname AIILOG.

- “Enabling event logging” on page 26
- “Log record structure” on page 27
- “Sample logs” on page 28
Enabling event logging

You can enable event logging to log all events, including system status events and security events.

Procedure

Set the Log parameter in the Distributed Access Infrastructure server configuration file to On, as shown in the following example.

```
Log(On) /* Log(Off|On)  Default: On */
```

If the Distributed Access Infrastructure server is active, you can change the logging status by issuing a z/OS MODIFY command. You can dynamically disable logging by issuing the following command:

```
F server_name,LOG OFF
```

You can dynamically enable or resume logging by issuing the following command:

```
F server_name,LOG ON
```

**Remember:** Distributed Access Infrastructure logs some events regardless of the logging state. For example, startup events and errors are recorded whether the logging state is set to On or Off.
Log record structure

Each log record is variable length and contains specific information, such as the date and time of the recorded event.

Each log record has the following format:

```
yyyy/mm/dd hh:mm:ss.th xxxxxxxxxxxxxxxx ss eeeeee text
```

- `yyyy/mm/dd hh:mm:ss.th`: The local date and time when the event was recorded.
- `xxxxxxxxxxxxx`: The name of the Distributed Access Infrastructure component that generated the log record. In the majority of situations, this name is the XCF member name. The name is blank for log records that are generated during initialization before the name is determined.
- `ss`: A sequence field. For single-line log entries, this field is always 00. For log entries that consist of multiple lines, this field is the line sequence number, which starts at 00.
- `text`: Text that describes the event that was logged. For records that consist of multiple lines, all text lines are indented except for the first line (sequence number 00).

For log records that consist of multiple lines, the same date, time, XCF member name, and event code are repeated in each record.
Sample logs

The sample logs provide examples of different recorded events. You can compare these samples with your own logs to understand the events that are being recorded.

Server startup logging

During initialization, the Distributed Access Infrastructure servers unconditionally generate startup, environment, and configuration log records, as shown in the following example:

```
2009/12/14 11:49:20.55 00 STARTUP Distributed Access Infrastructure V1.1.0
2009/12/14 11:49:20.55 01 STARTUP Tools Access Server initialization started
2009/12/14 11:49:20.55 TAS###EC05003E 00 STARTUP Environment:
2009/12/14 11:49:20.55 TAS###EC05003E 01 STARTUP Job.....DAITAS System...EC05 ASID.....003E
2009/12/14 11:49:20.55 TAS###EC05003E 02 STARTUP User.....USRT001 Group.....SYS1 JobNum.....000000079
2009/12/14 11:49:20.55 TAS###EC05003E 03 STARTUP Local....GMT-O8 GMT......2009/12/14 19:49
2009/12/14 11:49:20.55 TAS###EC05003E 00 PreLoad AIICOM 00000700 AIICOM+20091129+13.34 V1.1.0
2009/12/14 11:49:20.55 TAS###EC05003E 00 PreLoad AIICOMM 9182ACAC0 AIICM+20091129+13.34+00160
2009/12/14 11:49:20.55 TAS###EC05003E 00 PreLoad AIICMS 9182A230 AIIMSE+20091129+13.34+00160
2009/12/14 11:49:20.94 TAS###EC05003E 00 ConfgEXE Parameters given on Job EXEC
2009/12/14 11:49:20.94 TAS###EC05003E 01 ConfgEXE TYPE=TAS,AIlCGT=AllTAS,BPEG=AllTBPE
2009/12/14 11:49:20.94 TAS###EC05003E 01 ConfgEXE Parameter member name: AllTAS
2009/12/14 11:49:20.94 TAS###EC05003E 01 ConfgEXE Confg member name: AllTAS
2009/12/14 11:49:20.94 TAS###EC05003E 02 ConfgEXE CfgGroup(XAO(DalGroup)) /* Xcf group name */
2009/12/14 11:49:20.94 TAS###EC05003E 03 ConfgEXE ServerName(DAI Production TAS) /* Server name */
```

System status events

System status events comprise normal operating events such as component startup, component shutdown, and XCF join and leave status. The following example shows TAS joining the XCF group and all members in the group at the time the TAS joins:

```
2009/12/14 11:49:21.53 TAS###EC05003E 00 STARTUP XCF JOIN Group=DAIGROUP Member=TAS###EC05003E RC=00000000
2009/12/14 11:49:21.56 TAS###EC05003E 00 Members Current XCF member information
2009/12/14 11:49:21.56 TAS###EC05003E 01 Members NTWKTCPSEC050029 Active NTWK TCPSERV DAITCP EC03005
2009/12/14 11:49:21.56 TAS###EC05003E 02 Members TAS###EC05003E Active TAS DAITAS EC03005
```

As other members join and leave the XCF group, their status is recorded in the server log, as shown in the following example:

```
2009/12/14 11:58:58.06 TAS###EC05003E 00 Members SERVTESTEC0502 XCF Member Event=GEMSTATE System=EC03005 Job=TESTTOOL
2009/12/14 11:58:58.06 TAS###EC05003E 01 Members OldState=Not-Def NewState=Active Type=SERV ID=TESTSERV
```

Security Events

Security events show the connections that are established and terminated, the user logon ID on the established connection, and the success and failure of a client logon. The following example shows these events:

```
2009/12/14 17:25:21.44 NTWKTCPSEC730002A 00 STARTUP TCP communication starting, Port: 5124, Max connections: 18
2009/12/14 17:25:35.32 NTWKTCPSEC730002A 00 TcpInf TCP socket connected. Socket: 1, IP: 9.77.152.216
2009/12/14 17:25:38.82 NTWKTCPSEC730002A 00 Logon User logon, Socket: 1, User: USRT005
2009/12/14 17:25:38.86 NTWKTCPSEC730002A 00 Logon User passed security check: USRT005
2009/12/14 17:26:07.93 NTWKTCPSEC730002A 00 TcpInf TCP socket disconnect. Socket: 1, IP: 9.77.152.216, User: Nauser
2009/12/14 17:25:35.32 NTWKTCPSEC730002A 00 TcpInf TCP socket connected. Socket: 1, IP: 9.77.152.216
2009/12/14 17:25:38.82 NTWKTCPSEC730002A 00 Logon User logon, Socket: 1, User: USRT005
2009/12/14 17:25:38.86 NTWKTCPSEC730002A 00 Logon User passed security check: USRT005
2009/12/14 17:25:38.86 NTWKTCPSEC730002A 00 Logon User passed security check: USRT005
```

The following example shows an unsuccessful logon:

```
2009/12/14 06:32:26.54 NTWKTCPSEC730002B 00 Logon User logon, Socket: 1, User: USRT007
2009/12/14 06:32:26.64 NTWKTCPSEC730002B 00 ErrorSeg AIITCP Request=VERIFY,ENVIR=CREATE ended with RC=00000008 Security system RC='X'00000000' Reason='X'00000000'.
```

Additional messages might be available in JOBLOG for job DAITCP ( Job090090)

```
2009/12/14 06:32:26.64 NTWKTCPSEC730002B 01 ErrorSeg Group=Target=DAITCP Dir=Tool
```

Additional messages might be available in JOBLOG for job DAITCP ( Job090090)

```
2009/12/14 06:32:26.64 NTWKTCPSEC730002B 02 ErrorSeg Cmt=ErrorSeg Module=AIITASSEC Status=00000000 Reason=00000010
```

IBM Tools Base: Distributed Access Infrastructure User's Guide and Reference
The previous logon error is accompanied by the following entry in the TCP Server job log:

06.32.26 JO800090 ICH4001 USER(USRT007) GROUP(SYS1) NAME(################) 175

175 LOGON/JOB INITIATION - INVALID PASSWORD

06.32.26 JO800090 IRR0311 VERIFICATION FAILED. INVALID PASSWORD GIVEN.

Subordinate Tools Access Server (SOT) execution

The following example shows the execution of the assembler (ASMA90) in an SOT. The Ready lines are generated when the SOT is ready to accept new work.

The log entries show the following information:
- All allocations that were completed by the SOT before it invoked the program. These allocations are freed when the program ends.
- The program that is invoked and the parameters that are passed to it.
- The return code of the program or an abend code if the program abends.

Distributed Access Infrastructure output message statistics

Tool errors

The following example shows that an unsupported tool was requested:

2009/12/04 09:25:51.91 TASS+++++ECOS003E 02 Routing Message cannot be routed

2009/12/04 09:25:51.91 TASS+++++ECOS003E 02 Routing User=USRT005 Group=SYS1 Target=ECOS003E Dir=Tool

Correlator=C3969996 9381A430

2009/12/04 09:25:51.91 TASS+++++ECOS003E 03 Routing Cmt=Routing Module=AIITSM51 Status=00000000 Reason=00000353

The following example shows an ITKB Server connection failure:

2009/12/04 12:04:54.41 TASS+++++ECOS003E 01 ITKB Con getRept Server=ITKBREP1 DDD=CDST01 DDD=CDST00A Rectype=D Product=02 Report=01 Suffix=00000000 Vers=00000001

2009/12/04 12:04:54.41 TASS+++++ECOS003E 01 ITKB Con User=USRT005 Group=SYS1 Target=AIITAS Dir=Tool

Correlator=C3969996 9381A340

2009/12/04 12:04:54.41 TASS+++++ECOS003E 03 ITKB Con Cmt=ITKB Con Module=AIITFSYV Status=00000000 Reason=00000811
Chapter 7. Troubleshooting

Distributed Access Infrastructure issues messages and codes that can help you to diagnose and correct problems that you experience with the product.

Topics:

* "Runtime error messages (All)" on page 32
* "Abend codes" on page 44
* "Gathering diagnostic information" on page 47
Runtime error messages (AII)

Distributed Access Infrastructure issues messages that can help you understand the
status of the infrastructure and help you resolve errors.

Message format

Distributed Access Infrastructure messages adhere to the following format:
AIInnnnx

Where:

AII Indicates that the message was issued by Distributed Access Infrastructure
nnnn Indicates the message identification number
x Indicates the severity of the message:
A Indicates that operator intervention is required before processing
can continue.
E Indicates that an error occurred, which might or might not require
operator intervention.
I Indicates that the message is informational only.
W Indicates that the message is a warning to alert you to a possible
error condition.

Each message also includes the following information:

Explanation:
The Explanation section explains what the message text means, why it
occurred, and what its variables represent.

System action:
The System action section explains what the system will do in response to
the event that triggered this message.

User response:
The User response section describes whether a response is necessary, what
the appropriate response is, and how the response will affect the system or
program.

AII0001I  DAI Server is starting
Explanation:  One of the Distributed Access
Infrastructure servers (the TCP Server or the TAS Server) is starting.
System action:  Distributed Access Infrastructure
processing continues.
User response:  No action is required.

AII0003I  Server tasks initialization is in progress
Explanation:  The internal servers for each Distributed
Access Infrastructure Server are starting.
System action:  Distributed Access Infrastructure
processing continues.
User response:  No action is required.

AII0005I  Server task initialization has completed
Explanation:  The internal servers for each Distributed
Access Infrastructure Server completed initialization.
System action:  Distributed Access Infrastructure
processing continues.
User response:  No action is required.

AII0006I  Server joined the XCF group
Explanation:  The Distributed Access Infrastructure
Server successfully joined its XCF group. The XCF
group name is specified in the XcfGroupName
configuration parameter of the Distributed Access
Infrastructure Server.
**User response:** No action is required.

---

**Explanation:** Key 7 was not executed in storage for the Distributed Access Infrastructure TCP and TAS Servers.

**System action:** The DAI server issues a U300-0A abend and terminates.

**User response:** Correctly define the Program Property Table (PPT) for Distributed Access Infrastructure in the active SCHEDxx member in PARMLIB. A sample PPT definition is provided in the Distributed Access Infrastructure sample library (SAIISAMP).

---

**Explanation:** When the Distributed Access Infrastructure Servers execute PGM=AIIC000, parameters are passed to this program in the following format: keyword=value. The TYPE keyword parameter is required, and the value of the parameter specifies which server is being started. The only valid TYPE values are TCP and TAS.

**System action:** The Distributed Access Infrastructure Server issues a U300-1E abend and terminates.

**User response:** Specify either TYPE=TCP or TYPE=TAS in the EXEC statement parameters in the Distributed Access Infrastructure Server JCL.

---

**Explanation:** This error is an internal Distributed Access Infrastructure error.

**System action:** Depending on when and where Distributed Access Infrastructure processing detects this condition, Distributed Access Infrastructure can take various actions.

**User response:** Contact IBM Software Support.

---

**Explanation:** The client requested the services of a target tool that is not defined to Distributed Access Infrastructure.

**System action:** Distributed Access Infrastructure rejects the request and returns error information to the client.

**User response:** Reenter the request and specify a valid target tool.

---

**Explanation:** The client specifies a user ID that is not defined to the security system.

**System action:** TAS rejects the request and returns error information to the client.

**User response:** Reenter the request and specify a valid TAS service.

---

**Explanation:** Additional messages might be available in JOBLOG for JOB job_name (job_number) on system smf_id.

---

**Explanation:** This error can be caused by the following conditions:

- The client specifies a user ID that is not defined to the security system.
- The client specifies the incorrect password for the user ID.
- The SecurityGroup parameter is specified in the Distributed Access Infrastructure Server configuration, but the group is not defined to the security system.
- The SecurityGroup parameter is specified in the Distributed Access Infrastructure Server configuration, but the user ID is not connected to this group.
- The SecurityAppl parameter is specified in the Distributed Access Infrastructure Server configuration, and the specified application name is defined the APPL CLASS of the security system. However, the user ID does not have READ access to the APPL CLASS profile of the application.

This message provides the following information:

**action** The action is CREATE when Distributed Access Infrastructure is attempting to verify access of the client. The action is DELETE when Distributed Access Infrastructure detects an error while Distributed Access Infrastructure is cleaning up after processing.

**saf_rc** The return code from the SAF RACROUTE VERIFY request.

**sec_rc** The return code from the underlying security function (RACINIT).

**sec_rsn** The reason code from the underlying security function (RACINIT).
job_name

The job name of the Distributed Access Infrastructure Server.

job_number

The job number of the Distributed Access Infrastructure Server.

smf_id

The SMF ID of the system on which the server is running.

System action:  If this condition occurs while the user is attempting to log on, Distributed Access Infrastructure denies the logon request. If this condition occurs while attempting to access a z/OS resource, Distributed Access Infrastructure denies access to the resource. In all cases, an error is returned to the client.

User response:  See the return and reason codes, which are documented in the security systems RACROUTE reference manual. For example, for RACE, these codes are found in the z/OS Security Server RACROUTE Macro Reference (SA22-7692) in the “RACROUTE REQUEST=VERIFY” section.

AII0131E  A dynamic allocation error occurred.

Explanation:  The Distributed Access Infrastructure request requires the allocation of a z/OS data set, and that allocation failed.

This message provides the following information:

```
return_code
```

The DYNALLOC service return code.

error_code

The SVC 99 error code (S99ERROR) set by the DYNALLOC service.

info_code

The SVC 99 information code (S99INFO) set by the DYNALLOC service.

System action:  The Distributed Access Infrastructure request that required access to the data set is not processed, and an error is returned to the client.

User response:  See the return, error, and info codes, which are documented in the z/OS Programming: Authorized Assembler Services Guide (SA22-7608) in the “Interpreting DYNALLOC Return Codes” section. Correct the data set, member, and volume serial number then resubmit the request.

AII0132E  A data set name was not specified.

Explanation:  The Distributed Access Infrastructure request requires the client to specify a z/OS data set. However, the data set name was not specified on the request.

System action:  The Distributed Access Infrastructure request that required access to the data set is not processed, and an error is returned to the client.

User response:  Reenter the request and specify the z/OS data set name.

AII0133E  A ddname was not specified.

Explanation:  This is an internal Distributed Access Infrastructure error.

System action:  The Distributed Access Infrastructure request that required access to the ddname is not processed, and an error is returned to the client.

User response:  Contact IBM Software Support.

AII0134E  DSORG=org - Data set must be physical sequential (PS, PSU) or partitioned (PO, POU).

Explanation:  The Distributed Access Infrastructure request requires the client to specify a z/OS data set that can be processed sequentially. However, the specified data set cannot be processed sequentially. The data set must be a physical sequential data set or a partitioned data set. For either data set, a member name must also be specified.

System action:  The Distributed Access Infrastructure request that required access to the data set is not processed, and an error is returned to the client.

User response:  Reenter the request and specify the name of a z/OS data set that can be processed sequentially.
**AI0134E**  The data set is partitioned, but a member was not specified.

**Explanation:** The Distributed Access Infrastructure request requires the allocation of a z/OS data set. The client request specified a partitioned data set but did not specify a member name.

**System action:** The Distributed Access Infrastructure request that required access to the data set is not processed, and an error is returned to the client.

**User response:** Specify a member name for the Distributed Access Infrastructure request then resubmit the request.

**AI0140E**  A ddname was not specified.

**Explanation:** This error is an internal Distributed Access Infrastructure error.

**System action:** Processing continues.

**User response:** Contact IBM Software Support.

**AI0141E**  Data sets with fixed record or non-spanned variable record formats are supported. Input data set has an unsupported record format (DCBRECFM=recfm_flag).

**Explanation:** The Distributed Access Infrastructure request requires the client to specify a z/OS data set that can be processed by using record I/O. However, the specified data set has a record format that cannot be processed by using sequential record I/O.

**System action:** The Distributed Access Infrastructure request that required access to the data set is not processed. An error is returned to the client.

**User response:** Reenter the request and specify the name of a z/OS data set that can be processed by using sequential record I/O.

See DCBRECFM in SYS1.MACLIB(DCBD) to interpret the RECFM flags.

**AI0142E**  Data set OPEN failed with return code return_code.

**Explanation:** The Distributed Access Infrastructure request requires the client to specify a z/OS data set. Distributed Access Infrastructure attempted to OPEN the data set, but the OPEN failed without abending. The return code refers to the OPEN return code.

**System action:** The Distributed Access Infrastructure request that required access to the data set is not processed, and an error is returned to the client.

**User response:** See the return code to determine problem. Correct the OPEN failure then reenter the Distributed Access Infrastructure request.

**AI0143E**  ABEND aaaa_rr occurred during data set OPEN. Additional messages might be available in JOBLLOG for JOB job_name (job_number) on system smf_id.

**Explanation:** An abend occurred when Distributed Access Infrastructure attempted to OPEN the client-specified z/OS data set. This message provides the following information:

- **aaa_rr** The abend and reason code of the error that occurred when Distributed Access Infrastructure attempted to OPEN the data set.
- **job_name** The job name of the Distributed Access Infrastructure Server.
- **job_number** The job number of the Distributed Access Infrastructure Server.
- **smf_id** The SMF ID of the system on which the server is running.

**System action:** The Distributed Access Infrastructure request that required access to the data set is not processed, and an error is returned to the client.

**User response:** See abend and reason codes to determine the problem. Correct the problem then resubmit the Distributed Access Infrastructure request.

**AI0144W**  Text reading stopped because limit_reason was reached or would be exceeded by the next record. Text limit=mmmmmm.

**Explanation:** Distributed Access Infrastructure functions that return data set or ITKB report content have a data transfer limit. This limit (mmmmmm) was exceeded and the returned data content was truncated.

If the limit_reason is data transfer limit, the data transfer was stopped by the Distributed Access Infrastructure implementation limit. If the reason is client's text limit, the limit that was specified on the Distributed Access Infrastructure request was exceeded.

**System action:** All requested text is not returned to the client. Distributed Access Infrastructure returns an amount of text that does not exceed the text limit. A truncation warning is returned to the client.

**User response:** If the limit_reason is client's text limit, increase the limit that is specified on the Distributed Access Infrastructure request. If the reason is data transfer limit, contact IBM Software Support about overriding this limit.
Internal error. An invalid request was passed to AIIUREAD. Request=xx

Explanation: This error is an internal Distributed Access Infrastructure error.
The hexadecimal request code is shown in the message.

System action: Distributed Access Infrastructure fails the request and returns error information to the client.
User response: Contact IBM Software Support.

The requested DISPLAY service, "DISPLAY xxxxxxx", is not known.

Explanation: A DISPLAY request was targeted to a Distributed Access Infrastructure server. However, the specified request is not a valid DISPLAY request.

System action: The DISPLAY request is not processed, and an error is returned to the client.
User response: Specify a valid DISPLAY request, then resubmit the Distributed Access Infrastructure request.

The requested ITKB service, "xxxxxxx", is not known.

Explanation: A request was made for IMS Tools Knowledge Base (ITKB) processing. However, the specified request is not a valid ITKB request.

System action: The ITKB request is not processed, and an error is returned to the client.
User response: Specify a valid ITKB request, then resubmit the Distributed Access Infrastructure request.

Error connecting to ITKB server (server). FUNC=INITIAL RC=return_code
Rsn=reason_code, optional text

Explanation: The Distributed Access Infrastructure request required IMS Tools Knowledge Base (ITKB) services. However, Distributed Access Infrastructure could not connect to the specified ITKB server. The FUNC=INITIAL return and reason codes show the cause of the connection failure.

The following additional ITKB information might be included in this message:
• HKT2300E No RECON entries in registry.
• HKT2301E Incorrect server name.
• HKT2302E Insufficient access authority to repository.
• Global Initial table already exists.

System action: The ITKB request is not processed, and an error is returned to the client.
User response: Correct the connection failure then resubmit the ITKB request.

The FUNC=INITIAL return and reason codes are internal to IBM and are not externally documented. If these codes are required to diagnose the connection error, contact IBM Software Support.

ITKB report OPEN failed. HKTXACC FUNC=OPEN(INPUT) RC=return_code
Rsn=reason_code.

Explanation: Distributed Access Infrastructure was unable to OPEN the client-requested IMS Tools Knowledge Base (ITKB) report. The FUNC=OPEN(INPUT) return and reason codes show the cause of the OPEN failure.

System action: The ITKB request is not processed, and an error is returned to the client.
User response: Correct the OPEN failure then resubmit the Distributed Access Infrastructure request.

The ITKB getList request could not be executed because the HKTZAPI module has not been LOADed. Validate the server's STEPLIB.

Explanation: The IMS Tools Knowledge Base (ITKB) HKTZAPI module could not be loaded. The ITKB getList function requires that an ITKB library that contains the HKTZAPI module is included in the STEPLIB of the server.

System action: The ITKB getList request is not processed, and an error is returned to the client.
User response: The HKTZAPI module is delivered in ITKB APAR xxxxxxx. Ensure that this APAR is applied in your SMP/E environment.

Also, ensure that the library that contains the HKTZAPI module is in the STEPLIB concatenation of the server that issued this message.

Zone decimal field, "xxxxxxx", contains non-numeric values.

Explanation: The Distributed Access Infrastructure request requires the client to specify a numeric value in zone decimal format. However, the specified value contains non-numeric characters (xxxxxxx).

System action: The Distributed Access Infrastructure request is not processed, and an error is returned to the client.
User response: Specify numeric values only in the zone decimal value, then resubmit the Distributed Access Infrastructure request.
Starting DAI_internal_server

Explanation: One of the internal Distributed Access Infrastructure Servers started initialization.

System action: Distributed Access Infrastructure processing continues.

User response: No action is required.

DAI_internal_server beginning initialization phase 1

Explanation: One of the internal Distributed Access Infrastructure Servers started phase 1 of the initialization.

System action: Distributed Access Infrastructure processing continues.

User response: No action is required.

DAI_internal_server beginning initialization phase 2

Explanation: One of the internal Distributed Access Infrastructure Servers started phase 2 of the initialization.

System action: Distributed Access Infrastructure processing continues.

User response: No action is required.

DAI_internal_server initialization has completed

Explanation: One of the internal Distributed Access Infrastructure Servers completed initialization.

System action: Distributed Access Infrastructure processing continues.

User response: No action is required.

TCP Services initialization has completed

Explanation: The TCP server has initialized, but no communication has started yet.

System action: Distributed Access Infrastructure processing continues.

User response: No action is required.

Starting TCP Communications

Explanation: Distributed Access Infrastructure clients can now connect to the TCP Server.

System action: Distributed Access Infrastructure processing continues.

User response: No action is required.
AII1305E  •  AII2020I

System action: The request is ignored, and an error is returned to the client.
User response: Ensure that the correct TCP client was used.

AII1305E  An invalid request was targeted to the TCP Server
Explanation: The TCP Server received an invalid request from the client.
System action: The request is ignored, and an error is returned to the client.
User response: Ensure that the correct TCP client was used.

AII1900I  TCP Services shutdown has completed
Explanation: The TCP/IP API of the TCP Server was shut down successfully.
System action: Distributed Access Infrastructure continues the TCP server shutdown.
User response: No action is required.

AII1901I  DAI_internal_server beginning termination phase 1
Explanation: One of the internal Distributed Access Infrastructure Servers has started phase 1 of the termination.
System action: Distributed Access Infrastructure shutdown processing continues.
User response: No action is required.

AII1902I  DAI_internal_server beginning immediate termination phase 1
Explanation: One of the internal Distributed Access Infrastructure Servers has started phase 1 of the immediate termination.
System action: Distributed Access Infrastructure shutdown processing continues.
User response: No action is required.

AII1903I  DAI_internal_server beginning termination phase 2
Explanation: One of the internal Distributed Access Infrastructure Servers has started phase 2 of the termination.
System action: Distributed Access Infrastructure shutdown processing continues.
User response: No action is required.

AII1905I  DAI_internal_server termination has completed
Explanation: One of the internal Distributed Access Infrastructure Servers completed termination.
System action: Distributed Access Infrastructure shutdown processing continues.
User response: No action is required.

AII2000I  Starting DAI_internal_server
Explanation: One of the internal Distributed Access Infrastructure Servers started initialization.
System action: Distributed Access Infrastructure processing continues.
User response: No action is required.

AII2001I  DAI_internal_server beginning initialization phase 1
Explanation: One of the internal Distributed Access Infrastructure Servers started phase 1 of the initialization.
System action: Distributed Access Infrastructure processing continues.
User response: No action is required.

AII2002I  DAI_internal_server beginning initialization phase 2
Explanation: One of the internal Distributed Access Infrastructure Servers started phase 2 of the initialization.
System action: Distributed Access Infrastructure processing continues.
User response: No action is required.

AII2005I  DAI_internal_server initialization has completed
Explanation: One of the internal Distributed Access Infrastructure Servers completed initialization.
System action: Distributed Access Infrastructure processing continues.
User response: No action is required.

AII2020I  Processing tool definitions from member member
Explanation: This informational message shows the PROCLIB member name where TAS obtains tool definition overrides. The member name is specified by the TAS TOOLDEF configuration parameter.
System action: TAS uses the PROCLIB member that is shown in the message.
User response: No action is required.

AII2021E Error reading tool definitions from member member

Explanation: The tool definition member that is specified by the TAS TOOLDEF configuration parameter is not in the PROCLIB data set.

System action: TAS issues a U800-23 abend and terminates.

User response: The TAS TOOLDEF configuration parameter specifies the tool definition member name. Specify this member in the data set that is allocated to the PROCLIB in the TAS JCL and then restart TAS.

AII2022E A tool name has not been established. Skipping to next TOOL definition record.

Explanation: In the tool definition member, overrides are associated with a tool name. The tool name is specified by using the TOOL keyword in column 1 of the tool definition member. Non-TOOL keywords were found before the TOOL keyword.

System action: TAS issues a U800-23 abend and terminates.

User response: Correct the tool definition override with the incorrect TOOL definition and then restart TAS.

AII2023E The Tool name is not known to TAS.

Explanation: In the tool definition member, overrides are associated with a tool name. The tool name that is specified by using the TOOL keyword is not a defined Distributed Access Infrastructure tool.

System action: TAS issues a U800-23 abend and terminates.

User response: Correct the tool definition override to a valid tool name and then restart TAS.

AII2024E Tag in columns 1 through 8 is not valid.

Explanation: The tool definition member has a tag-value format. The tag value that is coded in column 1 is not a valid tag.

System action: TAS issues a U800-23 abend and terminates.

User response: Correct the tool definition override with the invalid tag and then restart TAS.

AII2025E Maximum number of libraries was exceeded.

Explanation: In the tool definition member, five libraries can be associated with a tool name, which means that no more that five PGMLIB statements can follow the TOOL statement. This message indicates that this limit was exceeded.

System action: TAS issues a U800-23 abend and terminates.

User response: For the tool definition in error, specify no more than five PGMLIB statements after the TOOL statement and then restart TAS.

AII2029E TAS terminating due to error processing tool definition member.

Explanation: The TAS TOOLDEF configuration parameter specifies the member name. An error was encountered while processing this member. Another Distributed Access Infrastructure message provides additional details about this error.

System action: TAS issues a U800-23 abend and terminates.

User response: View the Distributed Access Infrastructure message that details the error. Correct the tool definition member and restart TAS.

AII2050I Starting SOT address space with job name job_name.

Explanation: This informational message indicates that TAS issued a start for an SOT address space.

System action: The SOT address space initializes and becomes ready to accept client work requests.

User response: No action is required.

AII2901I DAI_internal_server beginning termination phase 1

Explanation: One of the internal Distributed Access Infrastructure Servers has started phase 1 of the termination.

System action: Distributed Access Infrastructure shutdown processing continues.

User response: No action is required.

AII2902I DAI_internal_server beginning immediate termination phase 1

Explanation: One of the internal Distributed Access Infrastructure Servers has started phase 1 of the immediate termination.

System action: Distributed Access Infrastructure shutdown processing continues.
User response: No action is required.

**AII2903I**  
**DAI_internal_server beginning**  
**termination phase 2**

Explanation: One of the internal Distributed Access Infrastructure Servers has started phase 2 of the termination.

System action: Distributed Access Infrastructure shutdown processing continues.

User response: No action is required.

---

**AII2905I**  
**DAI_internal_server termination has completed**

Explanation: One of the internal Distributed Access Infrastructure Servers completed termination.

System action: Distributed Access Infrastructure shutdown processing continues.

User response: No action is required.

---

**AII2906E**  
**Job-name cannot connect to**  
**XCF-group-name XCF group as a**  
**DAI-server Server. A DAI-server Server**  
**is already active in the group.**

Explanation: The job noted in the message text is attempting to join an XCF groups as either a TAS or TCP Server, however an instance of the server is already active in the XCF group.

System action: The job that is attempting to join the XCF group issues the AII2906E message and then terminates with a U500 ABEND.

User response: Verify the XcfGroupName parameter in the DAI server’s configuration. Ensure that multiple instances of a server do not attempt to join an XCF group.

---

**AII3000I**  
**SOT job_name initialization is complete.**

Explanation: This informational message indicates that the SOT address space is ready to accept client work requests.

System action: SOT processing continues.

User response: No action is required.

---

**AII3101I**  
**Program program_name completed in**  
**job_name RC=X'return_code' User=user_ID**

Explanation: This informational message indicates that a program that was dispatched into an SOT ended without an abend. The message identifies the program that was executed, the SOT where it ran, the program completion code, and the client security system user ID.

System action: The SOT becomes ready to process new client tool requests.

User response: No action is required.

---

**AII3102I**  
**PGM=program ABEND Completion**  
**Code=code Reason=X'reason_code' User=user_ID**

Explanation: This informational message indicates that a program that was dispatched into an SOT ended with an abend. The message identifies the program that was executed, the ABEND code and reason code, and the client security system user ID.

System action: The SOT cleans up its environment and becomes ready to process new client tool requests.

User response: No action is required.

---

**AII3301I**  
**DAI Common Server Interface is executing for application_name**

Explanation: This informational message indicates that the client is requesting services from a non-Distributed Access Infrastructure server by using the Distributed Access Infrastructure Common Server Interface (CSI).

System action: Distributed Access Infrastructure prepares for communication between the requesting client and the application server.

User response: No action is required.

---

**AII3302I**  
**XCF join was successful. Group=group**  
**Member=member**

Explanation: A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. This informational message indicates that CSI has joined the application server XCF group on behalf of the client.

System action: Distributed Access Infrastructure prepares for communication between the requesting client and the application server.

User response: No action is required.
**AI3303I**  XCF disconnect was successful.
**Group**=group **Member**=member

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. This informational message indicates that CSI has disconnected the client connection to the application server XCF group.

**System action:** CSI processing continues on behalf of the client.

**User response:** No action is required.

**AI3304E**  DAI Common Server Interface is terminating due to AIIGET error.
**AIIGET** **RC**=return_code
**Reason**=reason_code

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The Distributed Access Infrastructure AIIGET service detected an error while processing a request message from the client. For RC=8 and Reason=12, CSI timed out while waiting for a message from the client.

**System action:** Distributed Access Infrastructure terminates the client and CSI session. The SOT becomes available for a new client tool request.

**User response:** If the AIIGET return and reason codes are codes other than RC=8 and Reason=12, contact IBM Software Support for more information about this error.

**AI3301I**  The message's request is not valid.
**Request**=request

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The client message requested an undefined CSI service.

**System action:** Distributed Access Infrastructure rejects the request and returns an error response to the requesting client.

**User response:** See message AI3301I to determine which tool is being accessed, and then contact IBM Software Support.

**AI3462E**  An error occurred in an XCF service.
**Service**=service **RC**=return_code
**Reason**=X‘reason_code’

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. CSI issued an XCF service that is displayed in the message on behalf of the client. The service did not execute successfully.

**System action:** An error response is returned to the requesting client.

**User response:** The XCF services and their return and reason codes are documented in MVS® Programming: Sysplex Services Reference. See the services return and reason codes to determine if you can resolve the error. If not, contact IBM Software Support.

**AI3466E**  The message's request requires an active conversation. **Request**=request

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The client message sequence is not consistent with the CSI protocol.

**System action:** Distributed Access Infrastructure rejects the request and returns an error response to the requesting client.

**User response:** See message AI3301I to determine which tool is being accessed, and then contact IBM Software Support.

**AI3463E**  During Discover Groups processing, no groups matched the clients prefix.

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The client requested a list of active XCF groups whose names match a specific pattern. No groups that match the pattern are active.

**System action:** An error response is returned to the requesting client.

**User response:** See message AI3301I to determine which tool is being accessed. Ensure that the application tools server address space is active. If the application server is active, contact IBM Software Support.

**AI3464I**  The request required action for a specific XCF member. The member is not known to CSI.

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The client requested CSI services as an XCF group member but did not use CSI services to join the group as the specified member.

**System action:** Distributed Access Infrastructure rejects the request and returns an error response to the requesting client.

**User response:** See the AI3301I message to determine which tool is being accessed, and then contact IBM Software Support.
**AII3468E**  
Incoming message does not have a feedback area.

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The request message that was sent to CSI is not properly formatted.

**System action:** Distributed Access Infrastructure rejects the request and returns an error response to the requesting client.

**User response:** See message AII3301I to determine which tool is being accessed, and then contact IBM Software Support.

---

**AII3469I**  
The queried group has no members.

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The client requested a list of XCF members in the XCF group of the application tool.

**System action:** An error response is returned to the requesting client.

**User response:** See message AII3301I to determine which tool is being accessed, and then contact IBM Software Support.

---

**AII3470E**  
The request message's target is not valid. Target=\texttt{\texttt{target}}

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The client request message did not correctly specify if the message must be processed by CSI or forwarded to the application server.

**System action:** Distributed Access Infrastructure rejects the request and returns an error response to the requesting client.

**User response:** See message AII3301I to determine which tool is being accessed, and then contact IBM Software Support.

---

**AII3471E**  
The required group name was not specified.

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The client request requires the name of the XCF group of application tool. The group name was not provided in the request message.

**System action:** Distributed Access Infrastructure rejects the request and returns an error response to the requesting client.

**User response:** See message AII3301I to determine which tool is being accessed, and then contact IBM Software Support.

---

**AII3472E**  
The requested XCF group, \texttt{'group'}, does not match pattern, \texttt{'pattern'}, required by application

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The application's Distributed Access Infrastructure tool definition indicates that its XCF group name must match a specific pattern. The client that is requesting application services specified a group name that does not match this pattern.

**System action:** Distributed Access Infrastructure rejects the request and returns an error response to the requesting client.

**User response:** See message AII3301I to determine which tool is being accessed. Ensure that the application server XCF group name conforms to the required format. If it does, contact IBM Software Support.

---

**AII3473E**  
Logon request was rejected. Client's XCF member is already logged onto application

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The client sent a logon request for the application after the client had already logged on.

**System action:** Distributed Access Infrastructure rejects the request and returns an error response to the requesting client.

**User response:** See message AII3301I to determine which tool is being accessed, and then contact IBM Software Support.

---

**AII3474E**  
Logon requests are not supported by application

**Explanation:** A client is using the Distributed Access Infrastructure Common Server Interface (CSI) to access a non-Distributed Access Infrastructure application server. The client sent a logon request for the application but the application does not support logons.

**System action:** Distributed Access Infrastructure rejects the request and returns an error response to the requesting client.

**User response:** See message AII3301I to determine which tool is being accessed, and then contact IBM Software Support.
which tool is being accessed, and then contact IBM Software Support.

**AII9000I** Termination scheduled

**Explanation:** The server received a stop request (P servername).

**System action:** Termination of the server starts.

**User response:** No action is required.

**AII9001I** Immediate termination scheduled (not implemented in this release)

**Explanation:** The server received an immediate stop request (F servername,stop immediate).

**System action:** Immediate termination of the server starts.

**User response:** No action is required.

**AII9003I** Address space cleanup completed

**Explanation:** Cleanup of the address space completed. A Distributed Access Infrastructure server enters address space cleanup if it abnormally terminates.

**System action:** Distributed Access Infrastructure shutdown processing continues.

**User response:** If you want to continue Distributed Access Infrastructure processing after the abnormal shutdown, restart the Distributed Access Infrastructure server.

**AII9005I** DAI Server ended

**Explanation:** All Distributed Access Infrastructure processing in the address space has completed.

**System action:** The Distributed Access Infrastructure server is no longer available.

**User response:** No action is required.

If you want to continue Distributed Access Infrastructure processing after the shutdown, restart the Distributed Access Infrastructure server.

**AII9006I** The server left the XCF group

**Explanation:** During initialization, the Distributed Access Infrastructure Server joined the XCF group that is specified by the Distributed Access Infrastructure Server XcfGroupName configuration parameter. The Distributed Access Infrastructure Server has now left the specified XCF group.

**System action:** Distributed Access Infrastructure shutdown processing continues.

**User response:** No action required.

**AII9153E** XcfGroupName configuration parameter has an invalid value.

**Explanation:** The XcfGroupName parameter value supplied in the server’s configuration file does not conform to the required format for Distributed Access Infrastructure’s XCF group names.

**System action:** The Distributed Access Infrastructure server terminates.

**User response:** Correct the XcfGroupName configuration parameter to conform to the required format. The XCF group name may be 7 or 8 characters with the following format:

'\'AII<SMF-ID><optional-char>'

**Example:**

'\'AIISYS1 '

If the SMF ID (as defined in SYS1.PARMLIB(SMFPRMxx)) is fewer than four characters, add the pound sign character(s) to fulfill the format requirements (7 or 8 character length). Example for SMF-ID='PRD':

'\'AIIPRD# '

Chapter 7. Troubleshooting 43
Abend codes

This reference section provides detailed information about Distributed Access Infrastructure (DAI) abend codes.

For each abend code, the following information is provided where applicable:

**Explanation:**
The Explanation section explains what the abend code means, why it occurred, and what its variable entry fields are (if any)

**System Action:**
The System Action section explains what the system does next

**User Response:**
The User Response section describes whether a response is necessary, what the appropriate response is, and how the response affects the system or program

---

**U100**

**Explanation:** A BPE service that was invoked by a Distributed Access Infrastructure server failed.

The following list explains each reason code:

- **01** AWE GET failed
- **05** AWE ENQ failed
- **14** BPEATTCH failed
- **19** BPELTCB failed
- **1E** BPELOADC failed
- **23** BPEPOST failed
- **28** BPETERM failed
- **2D** BPELAGET failed
- **32** BPELAREL failed

**System action:** The system abnormally ends the Distributed Access Infrastructure server.

**User response:** Restart the Distributed Access Infrastructure server. If the problem persists, contact IBM Software Support.

---

**U300**

**Explanation:** The Distributed Access Infrastructure server experienced a z/OS related error.

The following list explains each reason code:

- **0A** The server is not executing in key 7.
- **0F** Adding a Resource Manager definition failed.
- **10** Removing a Resource Manager definition failed.
- **1E** An invalid TYPE parameter was specified in the EXEC statement PARM value of the Distributed Access Infrastructure server.

**System action:** The system abnormally ends the Distributed Access Infrastructure server.

**User response:** Complete one of the following actions based on the reason code that was issued:

- **0A** Define the primary initialization module of Distributed Access Infrastructure (AIIC0000) in the Program Property Table (PPT), which is specified in the SCHEDxx PARMLIB member, and this definition must specify KEY(7).

  See the example PPT definition in member AIIPPT in the Distributed Access Infrastructure sample library (SAILISAMP).

- **0F** Restart the Distributed Access Infrastructure server. If the problem persists, contact IBM Software Support.

- **10** Restart the Distributed Access Infrastructure server. If the problem persists, contact IBM Software Support.

- **1E** Specify TCP or TAS for the TYPE parameter in
the EXEC statement PARM value of the Distributed Access Infrastructure server, as in
the following example:
EXEC PGM=A1IC0000, PARM=('TYPE=TCP',...)

Update the JCL of the server with a valid TYPE parameter and then restart the server.

**U400**

**Explanation:** An error occurred while Distributed Access Infrastructure was initializing or terminating.

The following list explains each reason code:

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>The BPE task initialization failed.</td>
</tr>
<tr>
<td>03</td>
<td>The Distributed Access Infrastructure server shutdown was requested before its initialization completed.</td>
</tr>
<tr>
<td>07</td>
<td>The BPE task termination failed.</td>
</tr>
<tr>
<td>0A</td>
<td>Trace initialization failed.</td>
</tr>
<tr>
<td>0F</td>
<td>Log initialization failed.</td>
</tr>
</tbody>
</table>

**System action:** The system abnormally ends the Distributed Access Infrastructure server.

**User response:** Complete one of the following actions based on the reason code that was issued:

1. View the JOB log for messages. Correct any errors then resubmit the job.
2. Restart the Distributed Access Infrastructure server. Ensure that the server is properly initialized before you attempt to stop it.
3. View the JOB log for messages. Correct any errors then resubmit the job.
4. Verify that a //AIITRACE DD statement is coded in the Distributed Access Infrastructure server JCL.
5. View the Distributed Access Infrastructure server JOBLOG and AIILOG and correct any errors.

If you cannot determine the problem, contact IBM Software Support.

**U700**

**Explanation:** The TCP Server encountered an unrecoverable error.

The following list explains each reason code:

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Internal error</td>
</tr>
<tr>
<td>05</td>
<td>Attach failed</td>
</tr>
<tr>
<td>06</td>
<td>Initialize failed</td>
</tr>
<tr>
<td>07</td>
<td>Init API failed</td>
</tr>
<tr>
<td>0A</td>
<td>Shutdown error</td>
</tr>
<tr>
<td>23</td>
<td>No TCP segment</td>
</tr>
</tbody>
</table>
26 No data segment
28 TCP send failed
32 TCP parameters are invalid. The server cannot start.

**System action:** The system abnormally ends the TCP Server.

**User response:** Complete one of the following actions based on the reason code that was issued:

01 If the problem persists, contact IBM Software Support.
05 If the problem persists, contact IBM Software Support.
06 If the problem persists, contact IBM Software Support.
07 Verify that TCP/IP is operational, and then resubmit the job.
   If the error reoccurs or if the TCP/IP is not operational, contact the TCP/IP administrator and notify the administrator of the problem.
0A If the problem persists, contact IBM Software Support.
23 This error is a client request error. Check client used.
26 This error is a client request error. Check client used.
28 Verify that TCP/IP is operational. If it is operational, resubmit the job.
   If the error reoccurs or if the TCP/IP is not operational, contact the TCP/IP administrator and notify the administrator of the problem.
32 View the JOB log for messages. Correct any errors then resubmit the job.

---

**Explanation:** TAS encountered an unrecoverable error.

The following list explains each reason code:

23 An error occurred while TAS was process the tool definition member.

**System action:** The system abnormally ends the TAS Server.

**User response:** Complete one of the following actions based on the reason code that was issued:

23 See the Distributed Access Infrastructure error message that accompanies this ABEND message to resolve this error.
Gathering diagnostic information

Before you report a problem with Distributed Access Infrastructure to IBM Software Support, gather the appropriate diagnostic information.

Procedure

Provide the following information for all Distributed Access Infrastructure problems:

- A clear description of the problem and the steps that are required to re-create the problem
- All messages that were issued as a result of the problem
- Product release number and the number of the last program temporary fix (PTF) that was installed
- The version of DB2/IMS that you are using and the type and version of the operating system that you are using

Provide additional information based on the type of problem that you experienced:

For online abends, provide the following information:

- A screen capture of the panel that you were using when the abend occurred
- The job log from the TSO session that encountered the abend
- The job log from the server
- A description of the task that you were doing before the abend occurred

For errors in batch processing, provide the following information:

- The complete job log
- Print output
- Contents of the data sets that were used during the processing
Notices

This information was developed for products and services offered in the U.S.A.

This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.
Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

**Trademarks**

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [http://www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)
Other company, product, and service names may be trademarks or service marks of others.

**Terms and conditions for product documentation**

Permissions for the use of these publications are granted subject to the following terms and conditions:

**Applicability:** These terms and conditions are in addition to any terms of use for the IBM website.

**Personal use:** You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

**Commercial use:** You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

**Rights:** Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

**Privacy policy considerations**

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies
and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

Index

A
accessibility
  overview  11

C
cookie policy  49, 51

D
documentation
  accessing  9
  sending feedback  9

L
legal notices
  cookie policy  49, 51
  notices  49
  product documentation terms and
  conditions  49
  trademarks  49, 50

N
notices  49

P
product documentation terms and
  conditions  49

R
reader comment form  9

S
screen readers and magnifiers  11
  service information  8
  summary of changes  2
  support information  8

T
technotes  9
  trademarks  49, 50