IBM IMS Tools Base for z/OS
1.7

Distributed Access Infrastructure User's Guide and Reference

SC27-9856-06

Note:

Before using this information and the product it supports, read the information in “Notices” on page 45.

Seventh Edition (September 2025)

This edition applies to Version 1.7 of IBM IMS Tools Base for z/OS (program number 5655-V93) and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces SC27-9856-05.

Contents

About this information

IBM IMS Tools Base for z/OS® Distributed Access Infrastructure (also referred to as Distributed Access Infrastructure) provides remote access to IMS Tools products.

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 IMS 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 refer to the IMS Tools Product Documentation web page for complete product documentation resources:

https://www.ibm.com/support/pages/node/712955

The IMS Tools Product Documentation web page includes:

- Links to IBM Documentation for the user guides ("HTML")
- PDF versions of the user guides ("PDF")
- Program Directories for IMS Tools products
- Technical articles from IBM Software Support
- White papers that describe product business scenarios and solutions

Chapter 1. Distributed Access Infrastructure overview

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

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

Distributed Access Infrastructure is a set of software components that enable distributed clients access to IMS Tools products through TCP/IP socket communication over IPv4 or IPv6 networks. Distributed Access Infrastructure acts as a key component in extending the availability of IMS Tools products 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 can send and receive messages to and from the IMS Tools products that the clients are authorized to access.

Topics:

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.

Revision markers follow these general conventions:

- Only technical changes are marked; style and grammatical changes are not marked.
- If part of an element, such as a paragraph, syntax diagram, list item, task step, or figure is changed, the entire element is marked with revision markers, even though only part of the element might have changed.
- If a topic is changed by more than 50%, the entire topic is marked with revision markers (so it might seem to be a new topic, even though it is not).

Revision markers do not necessarily indicate all the changes made to the information because deleted text and graphics cannot be marked with revision markers.

SC27-9856-06 - September 2025

Table 1. SC27-9856-06 updates

Description	Related APARs
The TCP server supports IPv6 communication. By specifying IPv6 for the IPVersion parameter in the TCP server configuration and activating the TCP server, the TCP server functions as an IPv6 application enabling IPv6 communication. The following topics have been updated: • Chapter 1, "Distributed Access Infrastructure overview," on page 1 • "Sample logs" on page 14	PH64088

SC27-9856-05 - July 2025

Table 2. SC27-9856-05 updates

Description	Related APARs
TAS failover support. Distributed Access Infrastructure (DAI) automatically switches to a backup TAS when the primary TAS stops. This failover capability helps minimize the impact of service interruptions that might be caused by TAS failures or other issues. The following topics are added or updated: • "Distributed Access Infrastructure architecture" on page 5 • New messages: AII2015I and AII2016I	PH66126

SC27-9856-04 - April 2025

Table 3. SC27-9856-04 updates

Description	Related APARs
Multiple TCP server support. Multiple TCP servers can be configured for an XCF group. This enhancement provides the capability to build high availability DAI server configuration by using sysplex distributor where incoming TCP connection requests are distributed using dynamic virtual IP addresses (DVIPA). The following topics have been updated: • "Distributed Access Infrastructure architecture" on page 5 • Message: "AII2906E" on page 32	PH65149

SC27-9856-03 - September 2024

Table 4. SC27-9856-03 updates

Description	Related APARs
Password phrase support. The TCP server supports password phrases. Users can use 9- to 100-characters long password phrases to authenticate with the TCP server. The following topic has been updated: "TCP server security" on page 11	PH62437

Table 4. SC27-9856-03 updates (continued)

Description	Related APARs
Documentation update: Table "Events for secure connections" in “Sample logs” on page 14	N/A

SC27-9856-02 - March 2024

Table 5. SC27-9856-02 updates

Description	Related APARs
Support of all TLS client authentication options provided by z/OS Communications Server Application Transparent Transport Layer Security (AT-TLS). The TCP server supports the AT-TLS ClientAuthType of SAFCheck to validate and map the client certificate to an associated user ID that is to be used for TCP server services. The following topics have been added or updated: • “Distributed Access Infrastructure architecture” on page 5 • “TCP server security” on page 11 • “Transport Layer Security and Secure Socket Layer connections” on page 12 • “Security events” on page 14 • Message “AII0120E” on page 21 • “Diagnostic aids for connection errors” on page 42	PH57652

SC27-9856-01 - May 2023

Table 6. SC27-9856-01 updates

Description	Related APARs
The fix for this APAR changes the installation and verification program (IVP) for Distributed Access Infrastructure (DAI) so that some of the verification tests in the IVP can be run by a user ID that uses a password phrase. The following topics have been added: • Messages AII7101E, AII7102E, AII7103E, AII7104E, and AII7105E	PH53375
Other documentation changes. The following topics have been added: • Messages AII7000I and AII7004I	N/A

SC27-9856-00 - July 2022

Table 7. SC27-9856-00 updates

Description	Related APARs
• Multiple TASs can run in the XCF group, provided that only one TAS runs on the same z/OS system. For details, see “Distributed Access Infrastructure architecture” on page 5. Also, message AII2906E is updated.	N/A

Table 7. SC27-9856-00 updates (continued)

Description	Related APARs
Information about starting and stopping Distributed Access Infrastructure has been merged to the *IMS Tools Base Configuration Guide*.	N/A

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 products
- 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 operates on any z/OS hardware environment that supports the required software.

Software prerequisites

Distributed Access Infrastructure is designed to operate with any version of z/OS that supports the version of IMS that you are running. All supported releases of IMS are supported by Distributed Access Infrastructure.

Distributed Access Infrastructure components

Distributed Access Infrastructure consists of three main components: a TCP server, a Tools Access Server, and a Subordinate Tools Access Server.

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 with the TCP server, 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 IMS Tools products that are enabled for distributed access. The TAS is responsible for reading incoming messages and routing the messages to the correct IMS Tools product.

Subordinate Tools Access Server

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

Distributed Access Infrastructure architecture

Distributed Access Infrastructure operates in a sysplex 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 restrictions and limitations apply when configuring these servers:

- All servers must belong to the same XCF group to communicate with each other using XCF communication.
- Multiple TCP servers can belong to an XCF group, but only one TCP server can run on a single z/OS system.
- Multiple TASs can belong to an XCF group.

  Note: When multiple TASs run on multiple z/OS systems where only one TAS runs on each z/OS system, each TAS serves as the primary server on its respective z/OS system. When multiple TASs run on a single z/OS system, the failover feature is enabled, with one TAS acting as the primary server and the others acting as backup servers. For more information, see the topic "Setting up multiple TASs for TAS failover" in the *IMS Tools Base Configuration Guide*.

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

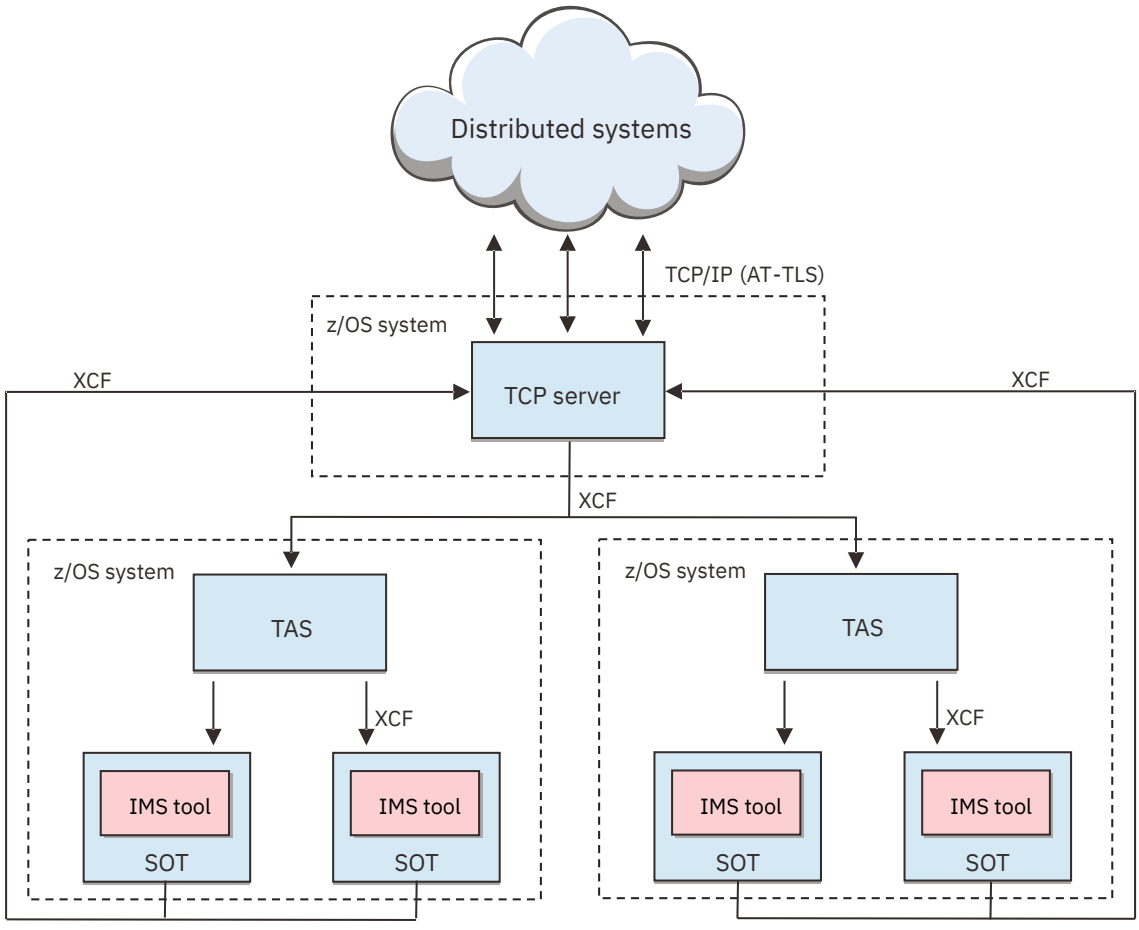

Figure 1. Distributed Access Infrastructure architecture

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 specified by the client 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.

You must use the *IMS Administration Foundation for z/OS* as the client. For more information, refer to *IBM Unified Management Server for z/OS User Guide*.

Service updates and support information

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

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

IBM Support: IMS Tools Base for z/OS

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

Always refer to the IMS Tools Product Documentation web page for complete product documentation resources:

https://www.ibm.com/support/pages/node/712955

The IMS Tools Product Documentation web page includes:

- Links to IBM Documentation for the user guides ("HTML")
- PDF versions of the user guides ("PDF")
- Program Directories for IMS Tools products
- Technical articles from IBM Software Support
- White papers that describe product business scenarios and solutions

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

http://www.redbooks.ibm.com

The IBM Information Management System website shows how IT organizations can maximize their investment in IMS databases while staying ahead of today's top data management challenges:

https://www.ibm.com/software/data/ims/

Receiving documentation updates automatically

To automatically receive emails that notify you when new technical articles 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 https://www.ibm.com/support/mynotifications
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 us provide the most accurate and highest quality information. If you have any comments about this information, see How to provide feedback in IBM Documentation.

When you provide feedback, include as much information as you can about the content you are commenting on, where we can find it, and what your suggestions for improvement might be.

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 IMS Tools Base components is provided in *IMS Tools Base Configuration Guide*.

See IMS Tools Base 1.7 Configuration Guide documentation.

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 products.

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 products 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 products.

Topics:

TCP server security

The TCP server authenticates a user by verifying a user credential.

The following types of user credentials are supported:

- Combination of a user ID and a password or a password phrase
- Combination of a user ID and a PassTicket
- Client certificate

Depending on how you want to manage access, you can additionally 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 or password phrase of the client or a client certificate that can be mapped to a user ID must be defined to the security system on the z/OS system where the TCP server is running.

If you use PassTicket instead of password for user authentication, you must define an APPL class profile for the TCP server and specify the SecurityAppl parameter. For details of PassTicket-based authentication, see the topic "Enabling RACF PassTicket" in the *IMS Tools Base Configuration Guide*.

Additional methods of controlling access to the TCP server

You can manage two types of security schemes to further restrict 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.

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 products that are enabled for distributed access.

Transport Layer Security (TLS) can provide security for communication between the IMS Tools products 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 on all sockets that might contain sensitive data.

Distributed Access Infrastructure TCP server can be enabled for TLS secure communication by using Application Transparent Transport Layer Security (AT-TLS) of z/OS Communications Server.

For AT-TLS policy setup for the TCP server port, see the topic "Configuring AT-TLS for secure communication" in the *IMS Tools Base Configuration Guide*.

Chapter 4. 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.

Topics:

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 nn eeeeeeee text
```

yyyy/mm/dd hh:mm:ss.th
The local date and time when the event was recorded.

xxxxxxxxxxxxxxxx
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.

nn
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.

eeeeeeee text
Abbreviation event name and 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:

```
2023/12/14 11:49:20.55                  00 STARTUP  Distributed Access Infrastructure V1.7.0
2023/12/14 11:49:20.55                  01 STARTUP    Tools Access Server initialization started
2023/12/14 11:49:20.55 TAS#####EC05003E 00 STARTUP  Environment:
2023/12/14 11:49:20.55 TAS#####EC05003E 01 STARTUP    Job.....DAITAS     System...EC05      ASID.....003E
2023/12/14 11:49:20.55 TAS#####EC05003E 02 STARTUP    User....USRT001    Group....SYS1      JobNum...STC00079
2023/12/14 11:49:20.55 TAS#####EC05003E 03 STARTUP    Local...GMT-08     GMT......2023/12/14 19:49
2023/12/14 11:49:20.55 TAS#####EC05003E 00 PreLoad  AIICDM   00007000 AIICDM+20231129+13.34  V1.7.0
2023/12/14 11:49:20.56 TAS#####EC05003E 00 PreLoad  AIICMSM  9182ACA0 AIICMSM+20231129+13.34+B0160
2023/12/14 11:49:20.56 TAS#####EC05003E 00 PreLoad  AIICMSEI 9182A330 AIICMSEI+20231129+13.34+B0160

2023/12/14 11:49:20.94 TAS#####EC05003E 00 ConfgEXE Parameters given on Job EXEC
2023/12/14 11:49:20.94 TAS#####EC05003E 01 ConfgEXE   TYPE=TAS,AIICFG=AIITAS,BPECFG=AIITBPE
2023/12/14 11:49:20.94 TAS#####EC05003E 00 ConfgMem Parameter member name: AIITAS
2023/12/14 11:49:20.94 TAS#####EC05003E 00 ConfgMem TAS configuration member contents
2023/12/14 11:49:20.94 TAS#####EC05003E 01 ConfgMem   XcfGroupName(DaiGroup)              /* Xcf group name  */
2023/12/14 11:49:20.94 TAS#####EC05003E 02 ConfgMem   TasServerName(DAI Production TAS)   /* Server name     */
2023/12/14 11:49:20.94 TAS#####EC05003E 03 ConfgMem   SecurityAppl(DAI)                   /* APPL CLASS 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:

```
2023/12/14 11:49:21.53 TAS#####EC05003E 00 STARTUP  XCF JOIN Group=DAIGROUP Member=TAS#####EC05003E RC=00000000
2023/12/14 11:49:21.56 TAS#####EC05003E 00 Members  Current XCF member information
2023/12/14 11:49:21.56 TAS#####EC05003E 01 Members    NTWKTCPSEC050029 Active   NTWK TCPSERV  DAITCP   EC03005
2023/12/14 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:

```
2023/12/14 11:58:58.06 TAS#####EC05003E 00 Members  SERVTESTEC05002A XCF Member Event=GEMSTATE System=EC03005  Job=TESTTOOL
2023/12/14 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 state of the connection, the user logon ID on the established connection, and the success and failure of a client logon.

The format of the IP address displayed in the event log depends on the Internet Protocol version that is used by the TCP server.

- If IPv4 is enabled, the IP address consists of four decimal numbers separated by periods. For example, 192.0.2.0.
- If IPv6 is enabled and the connection request is from an IPv6 client, the IP address consists of eight hexadecimal numbers separated by colons. For example, 2001:0DB8:0:0:0:0:0:0.
- If IPv6 is enabled and the connection request is from an IPv4 client, the IP address consists of six hexadecimal numbers separated by colons, followed by IPv4 IP address. For example, 0:0:0:0:0:FFFF:192.0.2.0.

The following examples show these events:

Events for non-secure connections

For a non-secure connection, a TCPIntf (TCP interface) message is displayed indicating that the connection is not secure.

```
2023/12/14 17:25:21.44 NTWKTCPSC753002A 00 STARTUP  TCP communication starting, Port: 5124, Max connections: 18
2023/12/14 17:25:21.44 NTWKTCPSC753002A 01 STARTUP    HOME IP: xxx.xxx.xxx.xxx, HOST NAME: SYSTEM1
2023/12/14 17:25:35.32 NTWKTCPSC753002A 00 TcpIntf  TCP socket connected.  Socket: 1, IP: xxx.xxx.xxx.xxx
2023/12/14 17:25:35.32 NTWKTCPSC753002A 00 TcpIntf  Connection is not secured for Socket: 1
2023/12/14 17:25:38.82 NTWKTCPSC753002A 00 Logon    User logon, Socket: 1, User: USRT005
2023/12/14 17:25:38.86 NTWKTCPSC753002A 00 Logon    User passed security check: USRT005
2023/12/14 17:26:06.30 NTWKTCPSC753002A 00 Logoff   User logged off: USRT005
2023/12/14 17:26:07.93 NTWKTCPSC753002A 00 TcpIntf  TCP socket disconnect. Socket: 1, IP: xxx.xxx.xxx.xxx, User: Nouser
2023/12/14 17:25:35.32 NTWKTCPSC753002A 00 TcpIntf  TCP socket connected.  Socket: 1, IP: xxx.xxx.xxx.xxx
2023/12/14 17:25:35.32 NTWKTCPSC753002A 00 TcpIntf  Connection is not secured for Socket: 1
2023/12/14 17:25:38.82 NTWKTCPSC753002A 00 Logon    User logon, Socket: 1, User: USRT005
2023/12/14 17:25:38.86 NTWKTCPSC753002A 00 Logon    User passed security check: USRT005
```

Events for secure connections

When a secure connection is established by using IBM z/OS Communications Server Application Transparent Transport Layer Security (AT-TLS), the TCP server examines the type of the connection, which is established based on AT-TLS policy statements. The type of the connection is written to the log as a security event after an event log for TCP socket connection establishment.

```
2023/12/14 17:25:35.32 NTWKTCPSC753002A 00 TcpIntf  TCP socket connected.  Socket: 1, IP: xxx.xxx.xxx.xxx
2023/12/14 17:25:35.32 NTWKTCPSC753002A 00 TcpIntf  ClientAuth SAFCheck on Socket: 1, certificate is mapped to the user USRT000
2023/12/14 17:25:38.82 NTWKTCPSC753002A 00 Logon    User logon, Socket: 1, User: USRT000
2023/12/14 17:25:38.86 NTWKTCPSC753002A 00 Logon    User passed security check: USRT000
2023/12/14 17:26:07.93 NTWKTCPSC753002A 00 TcpIntf  TCP socket disconnect. Socket: 1, IP: xxx.xxx.xxx.xxx, User: USRT000
```

When a connection is established successfully, one of the following event texts is written to the log. Internal ID `TcpIntf` is printed immediately before the event text indicating that the TCP interface was called.

Table 8. Event texts when a connection is established successfully

Event text	Meaning
Server Auth request on Socket: *nnnnnnnn*, server certificate is validated	• Server is set for the HandshakeRole parameter of the AT-TLS policy. • Server certificate is valid.
ClientAuth SAFCheck on Socket: *nnnnnnnn*, certificate is mapped to the user *uuuuuuuu*	• ServerWithClientAuth is set for the HandshakeRole parameter of the AT-TLS policy. • SAFCheck is set for the ClientAuthType parameter of the AT-TLS policy. • The certificate sent from the client has been validated and mapped to the user ID (*uuuuuuuu*).

Table 8. Event texts when a connection is established successfully (continued)

Event text	Meaning
Client Auth request on Socket: *nnnnnnnn*, AL-TLS ClientAuthType was PassThru	• ServerWithClientAuth is set for the HandshakeRole parameter of the AT-TLS policy. • PassThru is set for the ClientAuthType parameter of the AT-TLS policy. • Client certificate validation has been bypassed.
Client Auth request on Socket: *nnnnnnnn*, client certificate is validated	• ServerWithClientAuth is set for the HandshakeRole parameter of the AT-TLS policy. • Either Full or Required is set for the ClientAuthType parameter of the AT-TLS policy. • The certificate sent from the client has been validated.
Client Auth request on Socket: *nnnnnnnn*, client certificate was not received	• ServerWithClientAuth is set for the HandshakeRole parameter of the AT-TLS policy. • Full is set for the ClientAuthType parameter of the AT-TLS policy. • The certificate has not been validated because it was not presented by the client.
Connection is not secured for Socket: *nnnnnnnn*	AT-TLS is not used.

If an error is detected in the AT-TLS policy or in the client certificate, either of the following event logs is written. See “Diagnostic aids for connection errors” on page 42 to troubleshoot connection errors.

Table 9. Event texts when an error is detected in the AT-TLS policy or in the client certificate

Event text	Explanation	User response
An input message error Socket: *nnnnnnnn*, invalid format	The TCP server received a request message that it cannot interpret.	Ensure that Off is set for the ApplicationControlled parameter of the AT-TLS policy.
TCP socket connected. Socket: *nnnnnnnn*, IP: *www.xxx.yyy.zzz* TCP socket disconnect. Socket: *nnnnnnnn*, IP: *www.xxx.yyy.zzz*, User: Nouser	When an AT-TLS connection error occurs, only event logs indicating the establishment and termination of connections are logged.	Identify the cause of the error from the AT-TLS return code and correct the error. For more information, see the AT-TLS errors section in “Diagnostic aids for connection errors” on page 42.

The following example shows an unsuccessful logon:

```
2023/12/14 06:32:26.54 NTWKTCPSC753002B 00 Logon    User logon, Socket: 1, User: USRT007
2023/12/14 06:32:26.64 NTWKTCPSC753002B 00 ErrorSeg AII0120E RACROUTE REQUEST=VERIFY,ENVIR=CREATE ended with
                  RC=00000008 Security system RC=X'00000008'  Reason=X'00000000'.
                  Additional messages might be available in JOBLOG for JOB DAITCP   (JOB00090)
2023/12/14 06:32:26.64 NTWKTCPSC753002B 01 ErrorSeg   User=          Group=         Target=AIITCP  Dir=Tool
                  Correlator=00000000 00000000
2023/12/14 06:32:26.64 NTWKTCPSC753002B 02 ErrorSeg   Cmmt=ErrorSeg Module=AIINSSEC Status=00000000 Reason=00000810
```

The previous logon error is accompanied by the following entry in the TCP server job log:

```
06.32.26 JOB00090  ICH408I USER(USRT007 ) GROUP(SYS1    ) NAME(####################)  175
   175              LOGON/JOB INITIATION - INVALID PASSWORD
06.32.26 JOB00090  IRR013I  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 ends abnormally.
- Distributed Access Infrastructure output message statistics.

```
2023/08/17 13:06:48.23 SOT#0001EC05005C 00 Ready- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
2023/08/17 14:43:44.21 SOT#0001EC05005C 00 ToolExec SOT#0001 is processing program ASMA90   for user USRT005  Tool=ASMA90   Sess=005C0001 C88946E3 9AE16699
2023/08/17 14:43:44.22 SOT#0001EC05005C 00 ToolExec Alloc DD=SYSLIB  +00 (SYSLIB  ) DSN=SYS1.MACLIB                                VOL=RESPCK Source=AIIEXEC
2023/08/17 14:43:44.23 SOT#0001EC05005C 00 ToolExec Alloc DD=SYSLIB  +01 (SYS00001) DSN=USRT005.MACLIB                             VOL=DASD01 Source=AIIEXEC
2023/08/17 14:43:44.24 SOT#0001EC05005C 00 ToolExec Alloc DD=SYSIN       (SYSIN   ) DSN=SYS11290.T144344.RA000.SOT#0001.R0100123     VOL=SCR01  Source=AIISETUP
2023/08/17 14:43:44.25 SOT#0001EC05005C 00 ToolExec Alloc DD=SYSLIN      (SYSLIN  ) DSN=SYS11290.T144344.RA000.SOT#0001.R0100124     VOL=SCR01  Source=AIIEXEC
2023/08/17 14:43:44.26 SOT#0001EC05005C 00 ToolExec Alloc DD=SYSPRINT    (SYSPRINT) DSN=SYS11290.T144344.RA000.SOT#0001.R0100125     VOL=SCR03  Source=AIISETUP
2023/08/17 14:43:44.27 SOT#0001EC05005C 00 ToolExec Alloc DD=SYSADATA    (SYSADATA) DSN=SYS11290.T144344.RA000.SOT#0001.R0100126     VOL=SCR01  Source=AIISETUP
2023/08/17 14:43:44.28 SOT#0001EC05005C 00 ToolExec Alloc DD=SYSTERM     (SYSTERM ) DSN=SYS11290.T144344.RA000.SOT#0001.R0100127     VOL=SCR01  Source=AIISETUP
2023/08/17 14:43:44.29 SOT#0001EC05005C 00 ToolExec Text copied from AIIDATA to SYSIN     Lines copied: 0024
2023/08/17 14:43:44.33 SOT#0001EC05005C 00 ToolExec Invoking PGM=ASMA90   using Tasklib=n/a      Running in DAI data capture mode
2023/08/17 14:43:44.33 SOT#0001EC05005C 01 ToolExec   PARM=ADATA,RENT,NOOBJECT,NODECK,XREF(LONG),LIST(133),USING(NOWARN),FLAG(NOCONT),TERM
2023/08/17 14:43:44.50 SOT#0001EC05005C 00 ToolExec Program ASMA90   completed in SOT#0001.  RC=X'000004' User=USRT005  Sess=005C0001 C88946E3 9AE16699
2023/08/17 14:43:44.51 SOT#0001EC05005C 00 OutStats Message statistics: Data Sent=00013884 Segments=001 User=USRT005
2023/08/17 14:43:44.51 SOT#0001EC05005C 01 OutStats   Writes=00218 FeedBack=Y Write Err=0000 Msg=14434385 0111290F EE577F1E 0000001C
2023/08/17 14:43:44.55 SOT#0001EC05005C 00 Ready- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Tool errors

The following example shows that an unsupported tool was requested:

```
2023/12/14 09:25:52.57 TAS#####EC05003E 00 Routing  Message cannot be routed
2023/12/14 09:25:52.57 TAS#####EC05003E 01 Routing    AII0100E The requested target, "ESHLOADX", is not a known DAI enabled IMS Tool.
2023/12/14 09:25:52.57 TAS#####EC05003E 02 Routing    User=USRT005   Group=SYS1     Target=ESHLOADX Dir=Tool
                Correlator=C3969996 9381A340
2023/12/14 09:25:52.57 TAS#####EC05003E 03 Routing    Cmmt=Routing  Module=AIITSMSI Status=00000008 Reason=00003535
```

The following example shows an ITKB server connection failure:

```
2023/12/14 12:04:54.55 TAS#####EC05003E 00 ITKB Con getRept Server=ITKBREP1 DBD=CUST01 DDN=CUST01A RecType=U
                Product=UZ Report=01 Suffix=00000000 Vers=00000001
2023/12/14 12:04:54.55 TAS#####EC05003E 01 ITKB Con   AII0149E Error connecting to ITKB server (ITKBREP1).
                FUNC=INITIAL RC=00000028 Rsn=X'0000000C'. HKT2301E Incorrect server name.
2023/12/14 12:04:54.55 TAS#####EC05003E 02 ITKB Con   User=USRT005   Group=SYS1     Target=AIITAS   Dir=Tool
                Correlator=C3969996 9381A340
2023/12/14 12:04:54.55 TAS#####EC05003E 03 ITKB Con   Cmmt=ITKB Con Module=AIITSFSV Status=00000000 Reason=00000811
```

Chapter 5. 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 (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) is starting.

System action

Distributed Access Infrastructure processing continues.

User response

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

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.

System action

Distributed Access Infrastructure processing continues.

User response

None. This message is informational.

AII0007E Key 7 execution is required

Explanation

Key 7 was not executed in storage for the Distributed Access Infrastructure TCP server and the TAS.

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 SCHED*xx* member in PARMLIB. A sample PPT definition is provided in the Distributed Access Infrastructure sample library (SAIISAMP).

AII0009E An invalid TYPE=PARAMETER was specified

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.

AII0051E An invalid AWE function was queued to server

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.

AII0100E **The requested target, "*requested_tool_name*", is not a known DAI enabled IMS Tool.**

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.

AII0110E **The requested TAS service, "*requested_service*", is not known.**

Explanation

The client requested a TAS service that is not defined to TAS.

System action

TAS rejects the request and returns error information to the client.

User response

Reenter the request and specify a valid TAS service.

AII0120E **RACROUTE REQUEST=VERIFY, ENVIR=*action* ended with RC=*saf_rc* Security system RC=X'*sec_rc*' Reason=X'*sec_rsn*'. Additional messages might be available in JOBLOG for JOB *job_name* (*job_number*) on system *smf_id*.**

Explanation

Distributed Access Infrastructure could not authenticate the client. This condition can occur when the client is logging on to Distributed Access Infrastructure or when the client is attempting to access a resource on z/OS.

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.
- Mixed-case password is translated to uppercase because NoMixedCase is set for the Password parameter in the Distributed Access Infrastructure server configuration.
- 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 RACF, these codes are found in the topic "RACROUTE REQUEST=VERIFY" in *z/OS Security Server RACROUTE Macro Reference* (SA23-2294).

AII0121E A user ID was not provided.

Explanation

A request was made to authenticate a user ID, but the user ID was not specified.

System action

If this condition occurs while you are attempting to log on, Distributed Access Infrastructure denies the logon request. If this condition occurs while you are attempting to access a z/OS resource, Distributed Access Infrastructure denies access to the resource.

User response

Ensure that the client specified a user ID. If the client specified a user ID, this error might be an internal error. Contact IBM Software Support.

AII0122E An internal AIIUSAM parameter error occurred.

Explanation

This error is an internal Distributed Access Infrastructure error.

System action

Distributed Access Infrastructure denies the security request.

User response

Contact IBM Software Support.

AII0130E A dynamic allocation error occurred. DynAlloc RC=*return_code* S99Error=*error_code* S99Info=*info_code*

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 topic "Interpreting DYNALLOC return codes" in *z/OS MVS Programming: Authorized Assembler Services Guide* (SA23-1371).

Correct the data set, member, and volume serial number then resubmit the request.

AII0131E 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.

AII0132E A ddname was not specified.

Explanation

This error 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.

AII0133E **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.

AII0134E **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.

AII0140E **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.

AII0141E **Data sets with fixed record or non-spanned variable record formats are supported. Input data set has an unsupported record format (DCBRECFM=*recfm_flags*).**

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.

AII0142E **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.

AII0143E **ABEND *aaa_rr* occurred during data set OPEN. Additional messages might be available in JOBLOG 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.

AII0144W **Text reading stopped because *limit_reason* was reached or would be exceeded by the next record. Text limit=*nnnnnnnn*.**

Explanation

Distributed Access Infrastructure functions that return data set or ITKB report content have a data transfer limit. This limit (*nnnnnnn*) 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.

AII0145E **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.

AII0146E **The requested DISPLAY service, "DISPLAY *xxxxxxxx*", 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, and then resubmit the Distributed Access Infrastructure request.

AII0148E **The requested ITKB service, "xxxxxxxx", 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, and then resubmit the Distributed Access Infrastructure request.

AII0149E **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.

AII0150E **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 FUNC=OPEN(INPUT) return and reason codes are internal to IBM and are not externally documented. If these codes are required to diagnose the OPEN error, contact IBM Software Support.

AII0151E **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

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

AII0152E **Zone decimal field, "*xxxxxxxx*", 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 (*xxxxxxxx*).

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, and then resubmit the Distributed Access Infrastructure request.

AII1000I **Starting *DAI_internal_server***

Explanation

One of the internal Distributed Access Infrastructure servers started initialization.

System action

Distributed Access Infrastructure processing continues.

User response

None. This message is informational.

AII1001I ***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

None. This message is informational.

AII1002I ***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

None. This message is informational.

AII1005I ***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

None. This message is informational.

AII1008I **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

None. This message is informational.

AII1009I **Starting TCP Communications**

Explanation

Distributed Access Infrastructure clients can now connect to the TCP server.

System action

Distributed Access Infrastructure processing continues.

User response

None. This message is informational.

AII1200E **AiiNTcp TCP interface error. Routine: *IVP_routine* , Action: *action*, Rc=Minus, ErrNo= *TCP_error_number***

Explanation

The installation and verification program (IVP) ended with an error. The routine and action indicate the IVP routine and its action when the error occurred.

The return code Minus indicates a TCP error, and the error number is a system error code for socket calls.

System action

The IVP was not completed, and an error is returned to the client.

User response

See the information about system error codes for socket calls in the *IP Sockets Application Programming Interface Guide and Reference*, and then fix the error by following the Programmer's response for the error number that is provided in this message.

AII1301E **TAS Server cannot be located: RC=*return_code* Rsn=*reason_code***

Explanation

The TCP server cannot send request to the TAS.

System action

The request is ignored, and an error is returned to the client.

User response

Ensure that the TAS is running and that both the TAS and TCP servers are using the same XCF group.

AII1302E **XCF send from TCP Server failed: RC=*return_code* Rsn=*reason_code***

Explanation

The TCP server send request to the TAS failed.

System action

The request is ignored, and an error is returned to the client.

User response

Ensure that the TAS is still running.

AII1303E **The target segment cannot be located**

Explanation

The TCP server cannot locate the target that was specified in the message 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.

AII1304E **The target is TCP but the data segment cannot be located**

Explanation

The TCP server cannot locate the data segment that was specified in the message 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.

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.

AII1306E **The requested message is not recognized or unsupported by the IMS Tools TCP Server *job_name***

Explanation

The TCP server received a request message from the client in the new format. This request message is not supported in the Distributed Access Infrastructure 1.6 or earlier versions.

System action

The request is ignored, and an error is returned to the client.

User response

Ensure that the load library specified in the STEPLIB of the TCP server and the TCP client settings for connecting to the TCP server are correct.

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

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

AII2015I **Backup TAS started in standby mode**

Explanation

The backup TAS deferred initialization and is active in standby mode. When the primary TAS terminates, the backup TAS resumes initialization and takes over as the primary TAS.

System action

Continues to monitor the primary TAS.

User response

None. This message is informational.

AII2016I **Backup TAS is assuming the role of the Primary TAS**

Explanation

The backup TAS detected the termination of the primary TAS. The backup TAS resumed initialization to take over the role of the primary TAS.

System action

Distributed Access Infrastructure processing continues.

User response

None. This message is informational.

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

None. This message is informational.

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.

AII2043E **TAS *job_name* initialization has not yet completed**

Explanation

During the initialization job (*job_name*) of TAS, the TAS received a request message from the client.

System action

TAS rejects the request and returns an error response to the requesting client.

User response

Ensure that the TAS initialization is complete, and then reenter the request.

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

None. This message is informational.

AII2051I **TAS stopping SOT address space with job name *jobname*.**

Explanation

During TAS shut down, TAS stops each active SOT address space.

During periods of high workload, TAS might start additional SOT address spaces. When the workload decreases, TAS will stop SOT address spaces to bring their number down to the value specified in the SOTMIN configuration parameter.

This message is issued for each SOT being stopped. The job name indicates which SOT is being stopped.

System action

TAS signals the SOT that it should terminate.

User response

None. This message is informational.

AII2052E **TAS is waiting for SOT address spaces to start.**

Explanation

TAS starts the SOT address spaces during initialization and verifies that all SOTs have started.

If any SOT has not initialized, TAS issues this message, waits a minute, and rechecks the SOTs' initialization.

System action

TAS rechecks the SOT status once a minute for up to 15 minutes.

Message AII2052E is issued after each check.

If all SOTs have not initialized after 15 minutes, TAS issues the AII2053E message and terminates.

User response

Check for SOT address space errors (for example, JCL errors or abends).

Correct the problem that is causing the SOT failure and restart TAS.

AII2053E **TAS is terminating due to SOT address spaces failing to start.**

Explanation

TAS starts the SOT address spaces during initialization.

This message is issued if one or more SOT address spaces failed to initialize.

System action

If all SOTs have not initialized within 15 minutes, TAS terminates and ends abnormally with U800-28.

User response

Check for SOT address space errors (for example, JCL errors or abends).

Correct the problem that is causing the SOT failure and restart TAS.

AII2054E **TAS is terminating. An obsolete *DAI_internal_server* task was invoked.**

Explanation

Several DAI modules have been obsoleted. This message is issued if DAI attempts to invoke an obsolete module.

The message indicates which DAI service made the attempt to invoke this obsolete module.

System action

The DAI service terminates and ends abnormally with U800-32.

User response

Report this situation to IBM Software Support.

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

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

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 group as either a TAS or TCP server. However, an instance of the server is already active on the same z/OS system in the XCF group. It is possible to run multiple TCP servers or TASs in the XCF group, but only one of each can run on the same z/OS system.

System action

The job that is attempting to join the XCF group issues the AII2906E message and then terminates with abend code U500.

User response

Verify the XcfGroupName parameter in the DAI server's configuration. Ensure that multiple instances of a TCP server or a TAS on the same z/OS system 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

None. This message is informational.

AII3100I ***job_name*** **is processing program** ***program_name*** **for user** ***user_ID*** **Tool=*tool_name***

Explanation

This informational message indicates that new work has been dispatched into an SOT address space. This message identifies the SOT that is being used, the program that is run, the client security system user ID, and the Distributed Access Infrastructure tool name.

System action

The SOT invokes the requested program with the authorities of the client user ID.

User response

None. This message is informational.

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 run, 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

None. This message is informational.

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 run, 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

None. This message is informational.

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 an internal function called the Common Server Interface (CSI) of the Distributed Access Infrastructure.

System action

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

User response

None. This message is informational.

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

None. This message is informational.

AII3303I **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

None. This message is informational.

AII3304E **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.

AII3461E **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 AII3301I to determine which tool is being accessed, and then contact IBM Software Support.

AII3462E **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 *z/OS 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.

AII3463E **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 AII3301I to determine which tool is being accessed, and then contact IBM Software Support.

AII3464I **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 AII3301I to determine which tool is being accessed. Ensure that the application tools server address space is active. If the applications server is active, contact IBM Software Support.

AII3466E **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 AII3301I 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. Ensure that the application tools server address space is active. If the application server is active, contact IBM Software Support.

AII3470E **The request message's target is not valid. Target=*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, '*group*', does not match pattern, '*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.

AII7000I **DAI version *vrm* SSI initialization complete**

Explanation

Initialization of the Distributed Access Infrastructure subsystem interface routine is completed. The *vrm* within the message indicates the version and release of this routine.

System action

The Distributed Access Infrastructure subsystem interface processing continues.

User response

None. This message is informational.

AII7004I **DAI SSI previously established is disabled**

Explanation

The subsystem interface for Distributed Access Infrastructure has been reinitialized.

System action

The instance of the Distributed Access Infrastructure subsystem interface that was previously initialized is now disabled.

User response

None. This message is informational.

AII7101E **Target DAI group *XCF_group_name* not found**

Explanation

The installation and verification program (IVP) attempted to join the specified XCF group *XCF_group_name*, but the group was not found.

System action

The IVP ends with a return code of 8.

User response

Ensure that the Distributed Access Infrastructure server is started and that the XCF group name matches the name specified in the XcfGroupName configuration parameter.

AII7102E **No active TAS in XCF group *XCF_group_name***

Explanation

The installation and verification program (IVP) attempted to send a request to a TAS, but there was no active TAS in the specified XCF group *XCF_group_name*.

System action

The IVP ends with a return code of 8.

User response

Start TAS in XCF group *XCF_group_name*, which is specified in the XcfGroupName configuration parameter.

AII7103E **TAS failure detected**

Explanation

A TAS failure occurred after the installation and verification program (IVP) sent a request to a TAS but before receiving a response.

System action

The IVP ends with a return code of 8.

User response

Correct the problem that is causing the TAS failure, and restart the TAS.

AII7104E **SSI service failed for FUNC=*function*, RC=*return_code*, RSN=*reason_code***

Explanation

An error occurred while the installation and verification program (IVP) was trying to send an SSI service request to the Distributed Access Infrastructure.

In the message text, *function* is the name of the internal function of the SSI service that failed.

System action

The IVP ends with a return code of 8.

User response

Restart the subsystem interface for Distributed Access Infrastructure. If the problem persists, contact IBM Software Support.

AII7105E **DAI version *vrm* subsystem interface not found**

Explanation

The installation and verification program (IVP) attempted to build a subsystem interface environment, but the corresponding subsystem interface was not found. The *vrm* within the message indicates the version and release of the Distributed Access Infrastructure subsystem interface.

System action

The IVP ends with a return code of 8.

User response

Start the subsystem interface for Distributed Access Infrastructure.

AII9000I **Termination scheduled**

Explanation

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

System action

Termination of the server starts.

User response

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

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

None. This message is informational.

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 must start with "AII" and be followed by a 1- to 5-character alphanumeric string, as follows:

```
'AII<1- to 5-char>'
```

Example:

```
'AIIXGRP '
```

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.

U200

Explanation

The Distributed Access Infrastructure server experienced a memory management error.

The following list explains each reason code:

05
Cell Pool initialization failed

0A
Cell Pool get failed

0F
Cell Pool free failed

System action

The system abnormally ends the Distributed Access Infrastructure server.

User response

Increase the REGION size of the Distributed Access Infrastructure server and then restart it. 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 SCHED*xx* PARMLIB member, and this definition must specify KEY(7).

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

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=AIIC0000, 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:

01
The BPE task initialization failed.

03
The Distributed Access Infrastructure server shutdown was requested before its initialization completed.

07
The BPE task termination failed.

0A
Trace initialization failed.

0F
Log initialization failed.

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:

01
View the JOB log for messages. Correct any errors then resubmit the job.

03
Restart the Distributed Access Infrastructure server. Ensure that the server is properly initialized before you attempt to stop it.

07
View the JOB log for messages. Correct any errors then resubmit the job.

0A
Verify that a //AIITRACE DD statement is coded in the Distributed Access Infrastructure server JCL.

View the Distributed Access Infrastructure server JOBLOG and AIILOG and correct any errors.

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

0F
Verify that a //AIILOG DD statement is coded in the Distributed Access Infrastructure server JCL.

View the Distributed Access Infrastructure server JOBLOG and correct any errors.

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

U500

Explanation

An error occurred while processing a z/OS, BPE, or Distributed Access Infrastructure service.

The following list explains each reason code:

14
The Distributed Access Infrastructure server could not join the XCF group that was specified in its configuration member.

1E
The Distributed Access Infrastructure server encountered errors while processing its PROCLIB configuration member.

48
The Distributed Access Infrastructure server encountered an error while attempting to add error information to the message.

50
The Distributed Access Infrastructure server encountered errors while processing its configuration parameters.

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:

14
An AII2900E error message is also generated that shows the IXCJOIN return and reason codes. See the *z/OS MVS Programming: Sysplex Services Reference* for more information about the return and reason codes.

Determine the cause of the IXCJOIN failure, and then correct the error and restart the server.

1E
View the JOB log for messages. Correct any parameter errors then resubmit the job.

48
This error might be a memory error. Increase the REGION size of the Distributed Access Infrastructure server then restart the server. If the problem persists, contact IBM Software Support.

50
View the JOB log for messages. Correct any parameter errors then resubmit the job.

U700

Explanation

The TCP server encountered an unrecoverable error.

The following list explains each reason code:

01
Internal error

05
Attach failed

06
Initialize failed

07
Init API failed

0A
Shutdown error

23
No TCP segment

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.

U800

Explanation

TAS encountered an unrecoverable error.

The following list explains each reason code:

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

28
TAS terminated due to SOT address spaces failing to start.

32
TAS terminated because an obsolete DAI_internal_server task was invoked.

System action

The system abnormally ends the TAS.

User response

Refer to the Distributed Access Infrastructure error message that accompanies this abend message to resolve this error.

Diagnostic aids for connection errors

Use this topic to troubleshoot connection errors.

If the TCP server detects a connection error, information about the error is returned to the client and also written to the TCP server event log. For details of event log messages, see Chapter 4, “Event logging,” on page 13. Such error information includes a message identifier that you can use to identify the error cause from “Runtime error messages (AII)” on page 19.

Logon errors
If user authentication fails, a SAF message is written to the Distributed Access Infrastructure job log and message AII0120E is written to the event log. Look up these messages to diagnose the authentication error.

AT-TLS errors
When IBM z/OS Communications Server Application Transparent Transport Layer Security (AT-TLS) detects an error, the connection might be terminated with no notification to the client and you might not see any error message that has a message number in the TCP server event log. In this case, review other security event log messages that are described in “Security events” on page 14 and diagnose the connection error.

Security event logs
Review the AT-TLS connection status in the TCP server security event log. A message that indicates the AT-TLS connection error might be logged. For details, see “Security events” on page 14.

However, in most cases, information about AT-TLS connection errors is not passed on to the TCP server and, therefore, the TCP server cannot acknowledge AT-TLS errors. In this case, only events indicating the establishment and termination of connections are written to the TCP server event log. To identify the cause of the error, see the AT-TLS trace to check the AT-TLS return codes for associated AT-TLS events.

AT-TLS return codes
When an AT-TLS connection error occurs, AT-TLS error message EZD1287I is written to the TCPIP job log. This message contains the return code that indicates the AT-TLS processing event and error cause. Look up the meaning of the AT-TLS return code in the topic "AT-TLS return codes" in the *z/OS Communications Server: IP Diagnosis Guide*.

To have message EZD1287I written to the TCPIP job log, the level of AT-TLS tracing must be 1 or an odd number. To set AT-TLS trace level, see the topic "AT-TLS policy statements" in the *z/OS Communications Server: IP Configuration Reference*.

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 IMS that you are using and the type and version of the operating system that you are using
- The version, release, and PTF level of IMS Tools Base. You can obtain this information by running the Tools Base Diagnostics Aid. After running the Tools Base Diagnostics Aid, attach the Load Module APAR Status report that is generated by the Tools Base Diagnostics Aid. For more information about the Tools Base Diagnostics Aid, see the *IMS Tools Base Common Services User's Guide and Reference*.

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 US. This material might 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, MD-NC119
Armonk, NY 10504-1785
US

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

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 jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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 actual people or business enterprises 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.

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.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Index

Product Number: 5655-V93

SC27-9856-06