IBM Data Virtualization Manager for z/OS
Version 1 Release 1

Parameters Guide

SC27-9811-00

Contents

About this information

This information supports IBM Data Virtualization Manager for z/OS (5698-DVM) and contains information about the various parameters supported in Data Virtualization Manager.

Purpose of this information

This information describes the various parameters supported in the IBM Data Virtualization Manager for z/OS.

Who should read this information

This information is intended for z/OS users who use IBM Data Virtualization Manager for z/OS, and system programmers, and system administrators who are responsible for installing and customizing IBM Data Virtualization Manager for z/OS. The customization information is also of interest to application developers who want to understand how various customization and tuning actions might affect the performance of their applications.

How to send your comments to IBM

We appreciate your input on this documentation. Please provide us with any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

Important: If your comment regards a technical problem, see instead "If you have a technical problem" on page vii.

Send an email to comments@us.ibm.com.

Include the following information:

- Your name and address
- Your email address
- Your phone or fax number
- The publication title and order number:

  IBM Data Virtualization Manager for z/OS Parameters Guide
  GC27-8874-00
- The topic and page number or URL of the specific information to which your comment relates
- The text of your comment.

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

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

If you have a technical problem or question, do not use the feedback methods that are listed for sending comments. Instead, take one or more of the following actions:

- Visit the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

Chapter 1. Using started task parameters

This chapter describes how to modify the started task parameters that control the IBM Data Virtualization Manager for z/OS using the ISPF application depending on the function Data Virtualization Manager server is supporting.

Invoking the task application

Complete the following steps to invoke the AVZ task application.

Procedure

1. Start the ISPF application and go to the IBM Data Virtualization Manager for z/OS's Primary Option menu.
2. Select the option **C** for **AVZ Admin**.
3. Press **ENTER**.

Results
The following panel is displayed:

```
                        Server Management Menu                       SSID: AVZ9
Option  ===>
                                                                    More:     +

   1 ISPF Session    - Display and modify ISPF/AVZ session parameters
   2 AVZ Parms       - Display and modify AVZ main task parameters
   3 AVZ Blocks      - Display formatted AVZ control blocks
   4 AVZ Stats       - Display AVZ product statistics
   5 AVZ Tokens      - Display and control product tokens
   6 AVZ Modules     - Display product module information
   7 AVZ Tasks       - Display product tasks
   8 AVZ IP Tree     - Display the IP address tree
   9 AVZ Prcs Blks   - Display the Cross Memory Process Blocks
  10 AVZ RPC         - RPC Control Facility
  11 AVZ Copies      - Display information about each copy of the product
  12 AVZ Storage     - Display virtual storage information
  13 Trace Archive   - Server Trace Archive Facility
  14 AVZ Group       - Display all remote users in a group
  15 NLS Tables      - Display National Language Support tables
  16 Link            - Display Link Tables
  17 RRS             - Display RRS Facilities
  18 SOM             - Display and control Security Optimization and Managemant
```

Available commands

The Started Task Parameter application supports all four scrolling commands (UP, DOWN, LEFT, RIGHT) and their PF key equivalents or scroll bar equivalents. It also supports the primary SORT and LOCATE commands, as well as the REPORT command.

The REPORT command can be used to generate a list of all parameters (REPORT ALL), or just the parameters that have been changed since startup (REPORT CHANGED). The report is written to the ISPF LIST dataset. The report requires that ISPF LIST datasets have a minimum logical record length and line length of 72 characters. You can set the values using the ISPF SETTINGS dialog. To view the report, use the ISPF LIST command to close the current list dataset and use the ISPF browse to view the dataset and use ISPF facilities to browse, view or edit the dataset.

In addition, the ISPF application supports the line commands in the following table:

Line command	Description
D	Displays the parameters within the group.

Line command	Description
F	Formats the information for the selected row.
P	Prints the associated control block for the selected row.
S	Starts the control block browse sub-application.

Type the command to the left of the line and press ENTER. When a line command has completed its action, a note is placed in the NOTE column as a reminder that you issued the command.

Viewing Details about a Parameter

Complete the following steps to view parameter details.

Procedure

1. To the left of the parameter group you would like to view, type D, for display.
2. Press **ENTER**. The system will display the **Parameters** panel, showing a listing of all parameters in the selected parameter group as well as their default values.

   In this example, the **PRODIMS** group is displayed:

```
 ------------------------------ Parameters ----------------- Scr 1 Row 1 of 87
   LCs: D Display  E Edit  F Format  P Print CB  S Show CB

  Parameter                                        Parameter
  Description                                      Value
  ACTIVATE IMS/ODBA SUPPORT                        NO
  APPLICATION GROUP NAME                           'NONE'
  CHECK FOR NOMFS IN TRANSACTION                   NO
  CHECK IMS PSB USER ACCESS                        YES
  CONVERT NULLS TO BLANKS - IMS SERVER             NO
  CONVERT 3F TO THIS HEX VALUE                     X'3F'
  DDNAME USED TO ALLOCATE RESLIB                   'CCTLDD'
  DRA TERM TIMEOUT VALUE                           10
  DSNAME OF THE DRA RESLIB                         'IMS.IFA4.SDFSRESL'
  FAST PATH BUFFERS PER THREAD                     1
  FAST PATH OVERFLOW BUFFERS                       1
  FUNCTION LEVEL OF PRODUCT REGION                 X'03'
  IDENTIFY RETRY WAIT TIME                         60
  IMS DLI PARAMETER LIST LOCATION                  ABOVE
  IMS RCLASS VALUE                                 'IMS'
  IMS RECONNECT INTERVAL                           300 SECONDS
Command ===>                                              Scroll ===> PAGE
```

3. To the left of any particular parameter, type D to display more information. In the above example, more information about the parameter **ACTIVATE IMS/ODBA SUPPORT**is shown.
4. Press **ENTER**. The system will display the **Parameter Information** panel, showing an explanation of the chosen parameter:

```
 BROWSE    Parameter Information                  Line 0000000000 Col 001 064
******************************** Top of Data ********************************
PARM      IMSODBA

MESSAGE   ACTIVATE IMS/ODBA SUPPORT

EXPLAIN   The IMSODBA parameter controls whether the system will
          initialize the IMS/DB ODBA interface.
******************************** Bottom of Data *****************************
```

5. Use the **END** command, or press the **F3** key, to return to the **Parameters** panel.
6. To the left of any parameter, type F to view information about the parameter value.

   In thIS example, the parameter **ACTIVATE IMS/ODBA SUPPORT** is shown.

7. Press **ENTER**. Another **Parameter Information** panel appears, showing parameter name, description text, whether it is updatable or read-only, maximum and minimum values, and the parameter value.

```
 BROWSE    Parameter Information                   Line 0000000000 Col 001 061
******************************** Top of Data ********************************
Parameter Name                   IMSODBA
Description Text                 ACTIVATE IMS/ODBA SUPPORT
Group Name                       PRODIMS
Updatable Parameter              N
Read-Only Parameter              N
Maximum Value                    0
Minimum Value                    0
Parameter Counter                69
Last Update Timestamp
Set During Initialization        0
Changed During Initialization    0
Set After Initialization         0
Changed After Initialization     0
Last Update Userid
Parameter Value                  NO
****************************** Bottom of Data ******************************
```

8. Use the **END** command, or press the **F3** key to return to the **Data Virtualization Server Parameters** panel.

Adding a Started Task Parameter to IN00 File

This section describes on how to add or modify a new started task parameter to the Server IN00 file.

Procedure

1. From the **ISPF primary option menu**, select the option **3 Utilities** .
2. Choose the option **4 Dslist**.
3. Enter ***hlq*.EXECFB** in **Dsname Level**. *hlq* is the high level qualifier.
4. Type **V** next to the data set ***hlq*.EXECFB** to view the files under the dataset.

```
  Menu  Options  View  Utilities  Compilers  Help

DSLIST - Data Sets Matching CSD.AI38.EXECFB                      Row 1 of 13

Command - Enter "/" to select action                Message          Volume
-------------------------------------------------------------------------------
     V   CSD.AI38.EXECFB                                             SHP100
         CSD.AI38.EXECFB.BK012420                                    SHP114
         CSD.AI38.EXECFB.BK121419                                    SHP106
         CSD.AI38.EXECFB.CB                                          SHP119
         CSD.AI38.EXECFB.GW                                          SHP100
         CSD.AI38.EXECFB.NEW                                         SHP10D
         CSD.AI38.EXECFB.OLD                                         SHP10A
         CSD.AI38.EXECFB.RPW                                         SHP109
         CSD.AI38.EXECFB.STRESS.TEST                                 SHP100
         CSD.AI38.EXECFB.ZOS12                                       SHP112
         CSD.AI38.EXECFB.ZOS2                                        MIGRAT2
         CSD.AI38.EXECFB.ZOS3                                        MIGRAT2
         CSD.AI38.EXECFB.ZOS3.D090904                                SHP105
***************************** End of Data Set list *****************************
```

5. Find your server's IN00 files using the find command. In the following example, *XYZY* is the server ID.

```
. . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  Menu  Functions  Confirm  Utilities  Help

VIEW              CSD.AI38.EXECFB                      Row 0000001 of 0000925
           Name     Prompt       Size   Created          Changed          ID
_________ $A                        1  2004/04/19  2004/04/19 17:20:05 AI38OSI
_________ #H                        5  2000/06/27  2000/06/27 10:30:35 AI38JFF
_________ #SUB                     18  2000/06/27  2000/06/27 10:26:01 AI38JFF
_________ #USAGE                   48  2000/06/27  2000/06/27 10:46:23 AI38JFF
_________ @DB2IN0A                490  2003/04/08  2015/07/05 23:08:36 AI38RPW
_________ ADBAINEF                 53  2013/03/07  2013/03/07 15:05:58 AI38ADA
_________ ADBAINEY                205  2004/04/20  2015/07/05 23:08:36 AI38RPW
_________ ADBAINHL                786  2004/04/20  2015/07/15 18:24:05 AI38ADA
_________ ADBAIN00               1069  2004/04/20  2017/03/10 17:49:01 TSASH
_________ ADBC                     17  2010/03/04  2010/03/04 14:30:43 AI38GW2
_________ ADBCINEF                 48  1999/09/23  1999/09/23 17:33:47 AI38DEW
_________ ADBCINGW               1212  2006/05/06  2015/07/05 23:08:36 AI38RPW
_________ ADBCIN0#                283  2000/11/15  2015/07/05 23:08:36 AI38RPW
_________ ADBCIN00               1464  2005/04/01  2020/04/17 09:56:02 TS5837
_________ ADBCIN01                288  2001/07/18  2015/07/05 23:08:36 AI38RPW
_________ ADBCIN02                906  2008/01/16  2015/07/05 23:08:37 AI38RPW
Command ===> F XYZYIN00                                  Scroll ===> PAGE
```

6. Type *V* to open the IN00 file in a read mode or *E* to open the IN00 file in a write mode.
7. Find the suitable section to add a parameter. The sections are grouped under IMS, SMF, TRACEBROWSE, etc. In the following example, the parameter **SMFFULLSQL** is added under **SMF** section.

```
000403  /*-------------------------------------------------------------------*/
000404  /* SET SOME SMF PARAMETERS                                           */
000405  /*-------------------------------------------------------------------*/
000406   IF 1 = 1 THEN DO
000419    "MODIFY PARM NAME(SMFFULLSQL)         VALUE(YES)"
```

If you have opened the file using **E** or edit mode, the changes will be saved immediately.

Chapter 2. IBM Data Virtualization Manager for z/OS started task parameters

The parameters that control the IBM Data Virtualization Manager for z/OS may be modified depending on the function IBM Data Virtualization Manager for z/OS is supporting with the ISPF application. For more information, see Chapter 1, “Using started task parameters,” on page 1.

The started task parameters are initially defined using IBM Data Virtualization Manager for z/OS initialization EXEC, xVZyIN00. Some parameters however, can be modified after the product has been started.

The following sections provide details about the started task parameter groups, as well as each parameter contained in the group. The groups include:

PRODADABAS parameter group

Parameter name	Parameter description	Default value	Update	Output only
ADABAS	ADABAS SUPPORT ACTIVATED Controls whether ADABAS support is activated. The ADABAS module, ADALNK, must be present in the STEPLIB concatenation when this option is set.	YES	No	No
ADABASAUTOMAP	ADABAS AUTOMAPPING ACTIVATED Allows the user to turn off the automapping feature.	YES	Yes	No
ADABASAUTOMAPB2I	ADABAS AUTOMAPPING CONVERT B TO I Changes the format of B format fields to I format. B(2) becomes	NO	Yes	No
ADABASAUTOMAPU2P	ADABAS AUTOMAPPING CONVERT U TO 2P Changes the format of U format fields to P format.	NO	Yes	No
ADABASCORRELATIONIDS	ADABAS CORRELATION NAMES Supports Column Correlation Names. **Note:** Support of this may cause a conflict with earlier SQL that accepted a statement of the form: SELECT AA AB FROM EMPQA1. With this option set to N0, and on earlier releases of ADABAS Support, this selects two columns, AA and AB. With this option set to YES, AB is considered a correlation name for AA. Commas must be used to separate the two column names, as in SELECT AA, AB FROM EMPQA1, which produces the correct results in either case.	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
ADABASDATEFORMAT	ADABAS DATE FORMAT Specifies the format that the ADABAS date and time fields are to be presented to and sent from `Data Virtualization_ADABAS`. Valid types are: • OD: (ODBC format) yyyy-mm-dd • US: (USA format) yyyy/mm/dd • EU: (European format) dd.mm.yyyy • UK: (United Kingdom format) dd-mm-yyyy	US	Yes	No
ADABASDATETIMENULL	ADABAS ALLOW DATE/TIME NULLS Specifies whether ADABAS date and time fields are, when no data is present, to be returned as a null string or as all zeros in the format specified by the **ADABASDATEFORMAT** parameter.	NO	Yes	No
ADABASDMFSEC	ADABAS DMF SECURITY ACTIVATED Specifies if a resource rule has to be constructed consisting of the DMF map name.		NO	NO
ADABASXTIME	ADABAS EXTEND TIME FIELDS TO 1/10 SEC Returns TIME fields one decimal place - HH:MM:SS:T		YES	NO
ADABASAUTOCOMMITBIND	ADABAS AUTOCOMMIT BIND OPTION Enables the AUTOCOMMIT BIND option.	YES	YES	NO
ADABASDBIDSMF	ADABAS COMMAND STATISTICS SMF Enabling this parameter makes that one SMF record is written for every DBID accessed at the end of each session. The records contain command usage statistics.		YES	NO
ADABASSQLDATETIME	ADABAS SQL DATE FORMAT Specifies whether to bind ADABAS Date fields as SQL_CHAR or SQL_DATE.	NO	YES	NO

Parameter name	Parameter description	Default value	Update	Output only
ADABASETBTTARGET	ADABAS ET BT TARGET Controls Data Virtualization's list of ADABAS targets (up to 10) that have been accessed or updated during the client connection. When a COMMIT or ROLLBACK is performed, this parameter indicates to which ADABAS targets the COMMIT or ROLLBACK is issued. Valid values are: • A: Accessed and updated databases are in the list. The list is not cleared at COMMIT or ROLLBACK, and remains active for the duration of the clients session. • U: Only updated targets are included in the list. The list is cleared at COMMIT or ROLLBACK. • N: Never allow a user to update more than one database target during the client session. • O: Never allow a user to update more than one database target between commit or rollback points. **Note:** If any of the above conditions occur, a SQLException is raised.	O	No	No
ADABASISSUEC5	ADABAS ISSUE C5 COMMAND Sets the **ADABASISSUEC5** parameter to cause a C5 command record to be written to the PL0G file after each ET (commit) operation. This record contains the Session and Generic Assureds, LAN userid, and other Audit related information.	NO	Yes	No
ADABASPRUNEMUPE	ADABAS PRUNE RESULT SETS Specifies whether to bypass the default result set pruning of unneeded columns if an MU or PE field is specified with an (*), such as AI(*). Valid values are: • NO: No result set pruning takes place. • NOTCOUNT: Count columns are not pruned. • ALL: All possible columns are to be pruned.	NO	Yes	No
ADABASSECURITY	ADABAS SECURITY ACTIVATED Controls whether a resource rule is to be constructed consisting of DBID and file.	YES	No	No

Parameter name	Parameter description	Default value	Update	Output only
ADABASSETUSERID	ADABAS SET USERID OPTION Causes an OPEN to be performed for each DBID accessed which sets the user ID to *xxxxyyyy* where *xxxx* is the Data Virtualization Subsystem name and *yyyy* is the binary Virtual Connection ID. This user ID then appears in the ADABAS PLOG for audit purposes.	YES	Yes	No
ADABASUBINFOSIZE	ADABAS USER + REVIEW INFO SIZE Specifies the amount of space to be allocated for the User Information and Review Information combined in the ADABAS User Block.	256 BYTES	No	No
ADABASUID	ADABAS UID ADD3 ACTIVATED Controls whether the customer can see the client uid in the ADABAS control block ADDS3 fields.	NO	Yes	No
ADABASUPPERCASE	ADABAS UPPERCASE SQL Controls whether incoming ADABAS SQL statements are converted to uppercase before execution.	NO	Yes	No
READONLY	ADABAS READONLY ACTIVATED Controls whether SQL access for ADABAS allows update type requests.	NO	No	No
SCOMMANDSEARCHTIME	MAX S COMMAND SEARCH TIME Specifies the maximum amount of time permitted for the execution of an **SX** command.	0	Yes	No

PRODAPPCMVS parameter group

Parameter name	Parameter description	Default value	Update	Output only
CHECKCONVIDINTERVAL	CONVID TIMEOUT CHECKING INTERVAL Controls how often (in seconds) each convid is checked to see if the convid has timed out. If the convid has timed out, the conversation is deallocated and the entry in the conversation id table is removed.	15	Yes	No
IMSDEALLOCONVTIME	DEALLOC IMS CONV TIME VALUE Specifies the maximum allowable duration of inactivity for any conversation. The inactive period is defined as time expired since the last APPC/MVS call.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
IDMSCNVIDTBLSZ	IDMS CONVERSATION ID TABLE SIZE Specifies the size (in KB) of the table used to maintain the status of active conversations.	256	No	No
IDMSDEALLOCLOGIC	DEFAULT IDMS DEALLOCATE LOGIC Specifies if and when in the APPC/MVS conversation lifecycle the IDMS partner conversation should be deallocated. Valid values are: • NONE: Do not alter DEALLOC logic • RETURN: Deallocate upon return	NONE	Yes	No
IDMSDEALLOCONVTIME	DEALLOC IDMS CONV TIME VALUE Specifies the maximum allowable duration of inactivity for any conversation. The inactive period is defined as the number of seconds expired since the last APPC/MVS call.	900	Yes	No
IDMSLOCALLU	DEFAULT IDMS LOCAL LUNAME	NULL	Yes	No
IDMSMODENAME	DEFAULT IDMS MODE NAME	NULL	Yes	No
IDMSPARTNERLU	DEFAULT IDMS PARTNER LUNAME	NULL	Yes	No
IDMSRETURNCONTROL	DEFAULT IDMS RETURN CONTROL Specifies when control is to be returned to the local program in the context of session allocation.	SESSION	Yes	No
IDMSSECURITYNOPASS	IDMS SUPPORT ATB_SECURITY_PROGRAM_NOPASS REQ When set to YES, application programs can invoke APPC connect using the Data Virtualization-implemented **ATB_SECURITY_PROGRAM_NOPASS** option. When set to NO, this option is not allowed/supported. This connection option allows applications to specify a userid without a password.	NO	Yes	No
IDMSSECURITYTYPE	DEFAULT IDMS SECURITY TYPE Specifies the type of access information the partner LU uses to validate access to the partner program and its resources.	NONE	Yes	No
IDMSSYMDEST	DEFAULT IDMS SMBOLIC DEST NAME	NULL	Yes	No
IDMSSYNCLEVEL	DEFAULT IDMS SYNC LEVEL Specifies the synchronization levels of the local and partner TP.	NONE	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
IDMSTXNTIMEOUT	DEFAULT IDMS TXN TIMEOUT VALUE Limits the wait time (in seconds) for the completion of a transaction. If the transaction times out, a message is placed in the communication buffer to notify the client that a timeout has occurred.	0	Yes	No
IMSCNVIDTBLSZ	IMS CONVERSATION ID TABLE SIZE Specifies the size of the table used to maintain the status of active conversations.	256 KB	No	No
IMSCONVTYPE	DEFAULT IMS CONVERSATION TYPE Identifies the conversation type on which the service is invoked. The valid values are: • Basic: TPs format their data into seperate records, with record length and data specified before sending it. • Mapped: (Do not use) TPs rely on APPC to format the data that the TPs send. **Note:** Set this value to `Basic`, or omit it.	BASIC	Yes	No
IMSDEFAULTMAPNAME	DEFAULT IMS MAP NAME	DFSDSP01	Yes	No
IMSLOCALLU	DEFAULT IMS LOCAL LUNAME Specifies the name of the local LU from which the caller's allocate request is to originate. The ability to specify the local LU name allows the caller to associate its outbound conversations with particular LUs. The caller's address space must have access to the named LU. Otherwise, a parameter error return code is returned. This is the new local LU name specified in SYS1.PARMLIB(APPCPMxx). This parameter is optional; the default is to use the APPC base LU defined in SYS1.PARMLIB(APPCPMxx). **Note:** It is recommended that a separate local LU be defined for each Data Virtualization Server you have running using IMS/APPC. Application developers should be informed of which LU to use with which copy of the Data Virtualization Server. The APPC base LU works in most cases; however, using a separate local LU tends to be a more reliable request.	N281AIM1	Yes	No
IMSLUEE0	ACTIVATE DFSLUEE0 EXIT	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
IMSLUEE0ESCSEQ	DFSLUEE0 ESCAPE SEQUENCE	< %NE02%>	Yes	No
IMSMODENAME	DEFAULT IMS MODE NAME Specifies the mode name designating the network properties for the session to be allocated for the conversation. The network properties include, for example, the class of service to be used. The mode name value of SNASVCMG is reserved for use by APPC/MVS. If a mode name of SNASVCMG is specified on the Allocate service, the request is rejected with a return code of parameter error. If you specify a symbolic destination name in the symbolic destination name parameter, set mode name to blanks to obtain the mode name from the side information. If the partner LU is the same or on the same system as the local LU, mode name is ignored. If the partner LU is on a different system, and you do not specify a symbolic destination name, a blank mode name defaults to any mode in effect for the local and partner LUs, or causes a return code of parameter error.	BATCH	Yes	No
IMSPARTNERLU	DEFAULT IMS PARTNER LUNAME Specifies the name of the IMS LU defined in SYS1.PARMLIB(APPCPMxx).	N281AIMS	Yes	No
IMSQUEUEKEEPTIME	DEFAULT IMS ALLOC QUEUE KEEP TIME VALUE Specifies the duration (in seconds) inbound allocates are preserved on the allocate queue during a period in which no outstanding REGISTER FOR ALLOCATES are active.	3600	Yes	No
IMSRCVALLOCTIMEOUT	DEFAULT IMS RCVALLOC TIMEOUT VALUE Specifies the wait duration (in seconds) prior to returning to the caller if no inbound allocates match the filter criteria specified. This is when used in conjunction with an **IMSRECVALLOCTYPE** of TIMED.	0	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
IMSRECVALLOCTYPE	DEFAULT IMS RECEIVE ALLOC TYPE Specifies when control is to be returned to the caller. The options are `IMMEDIATE`, `TIMED`, and `WAIT`. • `IMMEDIATE` causes control to be returned immediately regardless of the state of the allocate queue. • `TIMED` results in control being returned to the caller when either the allocate queue contains an inbound request which matches the filter criteria specified, or when the wait interval has expired. • `WAIT` specifies that control is to be returned only upon an inbound allocate which matches the filter criteria.	IMMEDIATE	Yes	No
IMSRETURNCONTROL	DEFAULT IMS RETURN CONTROL Specifies when control is to be returned to the local program in the context of session allocation.	SESSION	Yes	No
IMSSECURITYNOPASS	SUPPORT ATB_SECURITY_PROGRAM _NOPASS REQUESTS Controls whether application programs may invoke an APPC connect using the Data Virtualization-implemented option of **`ATB_SECURITY_PROGRAM_NOPASS`**. When set to `NO`, this option is not allowed/ supported. This connection option allows applications to specify a userid, without a password.	NO	Yes	No
IMSSECURITYTYPE	DEFAULT IMS SECURITY TYPE Specifies the type of access information the partner LU uses to validate access to the partner program and its resources.	PROGRAM	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
IMSSYMDEST	DEFAULT IMS SMBOLIC DEST NAME Specifies a symbolic name representing the partner LU, the partner TP name, and the mode name for the session on which the conversation is to be carried. The symbolic destination name must match that of an entry in the side information data set. The appropriate entry in the side information is retrieved and used to initialize the characteristics for the conversation. If you specify a symbolic destination name, the partner LU name, mode name, and TP name are obtained from the side information. If you also specify values for the partner LU name, mode name, or TP name parameters on the Allocate service, these values override any obtained from the side information. The symbolic destination name in this field can be from 1 to 8 characters long, with characters from character set 01134. If the symbolic destination name is shorter than eight characters, it must be left-justified in the variable field, and padded on the right with blanks. To not specify a symbolic destination name, set the symbolic destination name parameter value to 8 blanks and provide values for the partner LU name, mode name, and TP name parameters.	NULL	Yes	No
IMSSYNCLEVEL	DEFAULT IMS SYNC LEVEL Specifies the synchronization levels of the local and partner TP.	NONE	Yes	No
IMSTXNTIMEOUT	DEFAULT IMS TXN TIMEOUT VALUE Limits the wait time (in seconds) for the completion of a transaction. If the transaction times out, a message is placed in the communication buffer to notify the client that a timeout has occurred.	0	Yes	No
MONITORAPPC/IDMS	MONITOR APPC/IDMS Specifies whether to monitor APPC/IDMS conversations.	NO	Yes	No
MONITORAPPC/MVS	MONITOR APPC/MVS Specifies whether to monitor APPC/MVS conversations.	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
REALTIMESUMMARY	IN MEMORY REALTIME SUMMARY COUNT Controls the number of APPC/MVS real-time summary records to keep in memory at one time. If this parameter is set to zero, no APPC/MVS real-time summary records are retained in memory. The APPC/MVS summary records kept in memory can be interactively displayed.	60	Yes	No

PRODCOMM parameter group

Parameter name	Parameter description	Default value	Update	Output only
ALTERNATEIPADDRESS1	ALTERNATE IP ADDRESS ONE Specifies an alternate IP address to bind to.	NULL	No	No
ALTERNATEIPADDRESS2	ALTERNATE IP ADDRESS TWO Specifies an alternate IP address to bind to.	NULL	No	No
BYPASSCOMPRESSION	BYPASS OUTBOUND DATA COMPRESSION Bypasses outbound data compression.	NO	Yes	No
CLIENTHOSTNAME	CLIENT HOST NAME DATA Specifies the Host: header to generate when sending a client HTTP request, if no Host: header is specified by the caller.	NULL	Yes	No
CLIENTREFERRER	CLIENT REFERRER DATA Specifies the Referrer: header to generate when sending a client HTTP request, if no Referrer: header is specified by the caller.	NULL	Yes	No
CLIENTUSERAGENT	CLIENT USER AGENT DATA Specifies the User-agent: header to generate when sending a client HTTP request, if no User-agent: header is specified by the caller.	NULL	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
CONNECTRETRYINT	CONNECT RETRY INTERVAL Controls how long (in seconds) the main product address space waits between attempts to connect to any of the TCP/IP subsystems. This field is specified in seconds.	300	Yes	No
CONNECTTIMEOUT	TCP/IP CONNECT READ TIMEOUT VALUE The timeout value for several host operations. The most important use is for Data Virtualization Direct to control how long the host waits for a client TCP/IP (IBM or Interlink) connection to complete. Data Virtualization Web Server uses the value to control how long it waits for each in-bound URL segment to be transmitted. Interlink TCP/IP code also uses this field as the timeout value for directory services requests.	20	Yes	No
DRAINREQUESTDATA	DRAIN REQUEST DATA BEFORE CLOSE When set to YES, this option causes WWW transaction threads to issue an additional receive just prior to closing an HTTP sessions. This option can be used to correct for an anomalous CRLF, unaccounted for by the “Content-length:” header, which is sometimes sent by Microsoft Internet Explorer browsers. For certain network configurations, closing the session prior to receiving these extra two bytes causes a reset to reach the downstream client before all response data has been received by the client. This appears at the user-agent as a session failure and the downstream client does not read the entire HTTP response. The problem has been seen only with Internet Explorer 5.00.29xxx version Web browsers. The default setting for this option is N0 for systems at z/OS Version 1.4. The default is YES for earlier operating systems releases.	NO	Yes	No
ALTERNATEIPV6ADDR1	ALTERNATE IPV6 ADDRESS ONE Specifies an alternate IP version 6 address to bind to.		NO	NO

Parameter name	Parameter description	Default value	Update	Output only
ALTERNATEIPV6ADDR2	ALTERNATE IPV6 ADDRESS TWO Specifies an alternate IP version 6 address to bind to.		NO	NO
BYPASSENDONEOC	BYPASS EMPTY BUFFER AT EOC Makes the empty buffer not to be sent to the client at the termination of the connection.		YES	NO
DRDALOGONTIMELIMIT	DRDA LOGON REQUEST TIME LIMIT Sets the time limit, in seconds, for a response made to a DRDA logon request. If the time limit expires before a response is received, the request is abandoned. The minimum value that can be set is 1 second, and the maximum is 120 seconds.		YES	NO
MONGOPORT	MONGODB TCP/IP MAIN PORT Sets the port number used to listen for inbound TCP/IP MongoDB client sessions. The port is not used if the MONGODB parameter is set to *NO*. The minimum value that can be set is 0 and the maximum value that can be set is 64535.	27017. Note that MongoDB will also use the port number 1000 higher than this port number to listen for HTTP requests.	NO	NO
MONGOSSLPORT	MONGODB TCP/IP MAIN SSL PORT Sets the port number used to listen for inbound TCP/IP MongoDB client connections. SSL encryption is used on this port when it is active. SSL is not activated if the port number is/ remains zero. Note that MongoDB will also use the port number 1000 higher than this port number to listen for HTTP SSL requests. The minimum value that can be set is 0 and the maximum value that can be set is 64535.		NO	NO
IDFPORT	IDF TCP/IP MAIN PORT Sets the port number used to listen for inbound TCP/IP DRDA application requestor sessions. The port is not used if the IDF parameter is set to NO. The minimum value that can be set is 0 and the maximum value that can be set is 65535.	50000	NO	NO

Parameter name	Parameter description	Default value	Update	Output only
IDFSSLPORT	IDF TCP/IP SSL PORT Sets the port number used to listen for inbound SSL TCP/IP DRDA application requestor sessions. The port is not used if the IDF parameter is set to NO. If this parameter is not explicitly set when IDF support is initialized, SSL encryption will not be used for IDF. The minimum value that can be set is 0 and the maximum value that can be set is 65535.		NO	NO
OEPIOPORTNUMBER	OE SOCKETS PORT PIO NUMBER Sets the port number used to listen for, and accept all inbound OE Sockets TCP/IP sessions. This port number should be reserved for exclusive use by the main product address space. Each copy of the main product address space will need its own separate port number if TCP/IP is being used. This port is only used for parallel I/O traffic.		NO	NO
ALLOWOPTNETBUFFERS	ALLOW UNCOMPRESSED VARIABLE LENGTH BUFFERS Controls the usage of uncompressed network buffers with variable length rows called CMBVs.	YES	YES	NO

Parameter name	Parameter description	Default value	Update	Output only
OEIPV6HOSTDOMAIN	OE SOCKETS IPV6 HOST DOMAIN NAME Specifies the fully qualified internet host domain name to be used by a server when constructing fully-qualified HTTP URLs and domain settings. This parameter is used only for OE Sockets TCP/IP Connections. In a mixed IPv4/IPv6 environment, this parameter specifies the IPv6 host domain name. It is not used unless OEIPV6 is set to *YES*. In a web services environment, the fully qualified domain name is used in construction of certain replies to requests. A web services client will use this fully qualified domain name in additional requests. In a HTTP-API environment, setting this parameter can have a significant impact on whether web browsers correctly store and re-transmit HTTP cookie values sent to it from the server. Many web browsers will not store HTTP cookies when the domain name is set unless the name contains at least 3 embedded periods (2 periods if the name ends with .com, .edu, .net, .org, .gov, .mil, or .int). Other browsers may fail to transmit cookies properly unless this name is entirely lower case. For this reason, the server will automatically convert any value you specify for this parameter to lower case, and will issue a warning message if it does not contain sufficient qualification.		YES	NO
OEIPV6	OE IPv6 SUPPORT Controls the usage of IPv6 OE sockets calls. If this parameter is set to *YES*, IPv6 I/O will be used with OE sockets.		NO	NO

Parameter name	Parameter description	Default value	Update	Output only
DRDAEXECUTETIMELIMIT	DRDA EXECUTION TIME LIMIT Specifies a time limit, in seconds, that Data Virtualization will wait for a response from DRDA after submitting SQL for execution. If no response is received within the specified time, the request is abandoned. The minimum value that may be set is 0 seconds. The maximum is 3600 seconds. If 0 is specified, Data Virtualization does not impose any time limit and will wait until a response is received.	0	Yes	No
DRDALOGONTIME	DRDA LOGON REQUEST TIME LIMIT Specifies the time limit, in seconds, that Data Virtualization will wait for a response to a DRDA logon request. If the time limit expires before a response is received, the request is abandoned. The minimum value that may be set is 1 second. The maximum is 120 seconds.	20	Yes	No
DVIPABINDALL	DYNAMIC VIPA BIND ALL ADDRESSES	NO	No	No
KEEPALIVE	HTTP PERSISTENT SESSION REUSE SUPPORT Determines whether the Data Virtualization Server honors Connection: and Keep-alive: headers for in-bound HTTP/1.0 requests. When set to YES, the Data Virtualization Server attempts to honor in-bound headers which request persistent session support. When set to N0, the Data Virtualization Server ignores such headers for all HTTP/1.0 requests.	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
KEEPALIVELIMIT	HTTP PERSISTENT SESSION RE-USE LIMIT Sets a limit on how many times an HTTP persistent session is left open for immediate re-use by the downstream user-agent. A small number is recommended when most downstream user-agents are desktop Web browsers. A larger number is recommended when the downstream user-agent is known to be a proxy server. A value in the range 1 to 512 may be specified. **Note:** This parameter is only used when persistent session support is enabled via the **KEEPALIVE** parameter.	4	Yes	No
KEEPALIVETIMEOUT	HTTP PERSISTENT SESSION RE-USE TIMEOUT Specifies how long to let persistent sessions wait for another HTTP request to arrive on a session kept open for reuse. The value is specified in milliseconds.	4000	Yes	No
LINKDISPLAYTYPE	TCPIP CLIENT LINK DISPLAY ARCHITECTURE Can be set to select the method used to track client IP connection information. When it is not set, the system selects the DEFAULT method and bases the organization upon the NETMODE used by the server. When set to LINK, the server organizes client IP connection information in a linear list and displays it using the ISPF LINKS display panel. When set to TREE, the server organizes client IP connection information in a four-level tree structure, based upon the dot-notation IP address. The information can be displayed using the ISPF IP TREE display panel.	DEFAULT	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
NETWORKADJUST	NETWORK BUFFER ADJUSTMENT FACTOR. Controls what fraction of the communication buffer should be reserved to allow for buffer overflow. If the field is set to 20, 1/20th of the buffer is reserved. If it is set to 5, 1/5th of the buffer is reserved. This value should be reduced if buffer overflow errors occur.	20	Yes	No
NETWORKBUFFERSIZE	MAXIMUM NETWORK I/O BUFFER SIZE Controls the size of the buffer used to receive blocks of data from the network. A failure occurs if a client application sends a buffer larger than the maximum size. This value should be raised to allow larger blocks of data to be sent to and from the client. Minimum Value: 0 Maximum Value: 67108864.	256 KB	No	No
OEASYNCIO	OE SOCKETS ASYNC I/O Controls whether Async OE Sockets calls should be used. Async I/O is faster than synchronous I/O. If set to YES, Async I/O is used with OE Sockets. If set to NO, Async I/O is not used with OE Sockets.	YES	No	No

Parameter name	Parameter description	Default value	Update	Output only
OEHOSTDOMAIN	OE SOCKETS HOST DOMAIN NAME Specifies the fully qualified internet host domain name to be used by this Server when constructing fully-qualified HTTP URLs and domain settings. The OEHOSTDOMAIN parameter is used only for OE Sockets TCP/IP connections. The IBMHOSTDOMAIN and ITCHOSTDOMAIN parameters set the MVS TCP/IP and Interlink TCP/IP host domains, respectively. In a Web Services environment, the fully qualified domain name is used in construction of certain replies to requests. A Web Services client then uses this fully qualified domain name in additional requests. In a Web Server environment, the setting of this parameter can have a significant impact on whether Web browsers correctly store and later re-transmit HTTP cookie values sent to it from this Server. Many Web browsers do not store HTTP cookies when the domain name is set unless the name contains at least 3 embedded periods (2 periods if the name ends with.com,.edu,.net,.org,.gov,.mil, or.int). Other browsers may fail to transmit cookies properly unless this name is entirely lower case. For this reason, the server automatically converts any value you specify for this parameter to lower case, and issues a warning message if it does not contain sufficient qualification.	NULL	Yes	No
OEKEEPALIVETIME	OE SOCKETS KEEPALIVE TIME Uses the TCP/IP keep alive facility to detect that a connection is likely no longer valid and force a disconnect. If no data is transferred on a connection in the interval coded here, then the connection is tested and if no response is received, it is disconnected and any resources using it are freed. The smaller the value, the sooner invalid connections are cleaned up. However, the possibility of disconnecting slow connections is greater.	15 MINUTES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
OELISTENQDEPTH	OE SOCKETS LISTEN QUEUE DEPTH Specifies the maximum length for the connection request queue created by for the LISTEN socket. This value cannot exceed the installation defined maximum that is specified in the SOMAXCONN statement specified in the TCP/IP profile.	10	Yes	No
OENLPORTNUMBER	OE NON-LOAD BALANCED PORT NUMBER Sets the port number used to LISTEN for, and ACCEPT all inbound encrypted OE Sockets TCP/IP sessions. This port number should be reserved for use only by the main product address space. Each copy of the main product address space needs its own port number if SSL over OE Sockets is being used. There is no default value for the SSL port number if the value is not set in the initialization EXEC.	0	No	No
OEPORTNUMBER	OE SOCKETS PORT NUMBER Sets the port number used to LISTEN for, and ACCEPT all inbound OE Sockets TCP/IP sessions. This port number should be reserved for exclusive use by the main product address space. Each copy of the main product address space needs its own separate port number if TCP/IP is being used. There is no default value for this port number if it is not set in the initialization EXEC. **Note:** The port number can be set to a string of “ANY”. This is a special value used to show that the system should assign an ephemeral port number for use by the product.	NULL	No	No

Parameter name	Parameter description	Default value	Update	Output only
OESSLPORTNUMBER	OE SOCKETS SSL PORT NUMBER Sets the port number used to LISTEN for, and ACCEPT all inbound encrypted OE Sockets TCP/IP sessions. This port number should be reserved for use only by the main product address space. Each copy of the main product address space needs its own port number if SSL over OE Sockets is being used. There is no default value for the SSL port number if the value is not set in the initialization EXEC.	0	No	No
OESTACK	OE SOCKETS TCP/IP STACK NAME Specifies the name of the OE TCP/IP stack that should be used. For OE TCP/IP, this parameter is optional. If this parameter is not set, then the default OE stack is used. If this parameter is used to select an OE TCP/IP stack, then the value must be one of the SUBFILESYSTYPE values specified in the BPXPRMxx PARMLIB member.	NULL	No	No
SOCKETLINGER	SOCKET LINGER TIME Indicates the socket linger time (in seconds) for IBM TCP/IP and IBM OE Sockets. If set to zero, socket linger is turned off. If set to a non-zero value, the socket linger is turned on and set for the number of seconds specified by this parameter.	20	No	No
VTAMEXITS	ENABLE VTAM SCIP/LOGON EXITS	NO	Yes	No
WSOEBALANCEDPORT	WEB SERVICES BALANCED PORT Specifies the port number used to listen for z/Services requests that can be balanced to group members.	0	No	No
WSOEPORT	WEB SERVICES OE PORT AND STUDIO HTTP PORT Specifies the port number used to listen for all inbound z/Services and Data Virtualization Studio requests.	0	No	No

Parameter name	Parameter description	Default value	Update	Output only
WSOESSLPORT	WEB SERVICES HTTP SSL PORT NUMBER Specifies the SSL-encrypted HTTP port used to listen for z/Services requests. These requests are not balanced to group members.		No	No

PRODEVENT parameter group

Parameter name	Parameter description	Default value	Update	Output only
DFHSM	DFHSM SUPPORT ENABLED IN SERVER Specifies whether the server should pre-initialize DFHSM support during start-up. If set to N0, no pre-initialization is performed and authorized DFHSM services are unavailable in the server. If set to YES, initialization is attempted, and if successful authorized DFHSM processing can be performed once start-up has completed. If errors are detected during initialization, warning message(s) are issued and DFHSM support is disabled. If disabled, no additional DFHSM processing of any kind, including clean-up of outstanding DFHSM MWE control blocks remaining after the last product shutdown is performed.	NO	No	No
DFHSMCLEANUPINTERVAL	DFHSM PENDING REQUEST CLEANUP INTERVAL Controls how often a check for pending inflight HRECALL requests is made. Requests which time out are abandoned by transaction subtasks but must be cleaned up. Failure to free the DFHSM MWE ECBs can leave below-the-line CSA storage areas permanently allocated. The interval value is specified in seconds and should be a factor of one hour. The value should divide evenly into 3600. The interval is automatically set to 3600 (1 hour) if DFHSM support is not enabled during start-up.	3600	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
DFHSMDRAIN	DFHSM DRAIN MODE IS IN EFFECT Can be set manually to prevent the Server from scheduling new HRECALL requests. The Server continues to monitor already inflight requests for completion, and free the associated MWE control blocks. The Server sets DFHSMDRAIN(YES) in effect if more than 125 pending HRECALL requests are outstanding. It then restores DFHSMDRAIN(NO) once the number of pending requests drops below 100, PROVIDING no manual change to DFHSMDRAIN or DFHSMSTATUS are made. Any manual change prevents the Server from automatically restoring full non-drain processing. **Note:** DFHSMDRAIN(NO) is always put in effect by the Server ANY time you manually set the DFHSMSTATUS parameter.	NO	Yes	No
DFHSMDRAINAUTO	SERVER SHOULD AUTO-RESET DFHSMDRAIN An output-only field which is set to YES only after the Server has changed DFHSMDRAIN to YES. While set to YES, the Server is responsible for resetting DFHSMDRAIN(NO) once sufficient HRECALL completions have been detected to allow new requests to be scheduled. Manually changing either DFHSMSTATUS or DFHSMDRAIN causes this field to be set to N0, and prevents the Server from resetting DFHSMDRAIN automatically.	NO	No	Yes
DFHSMSHUTDOWNWAIT	SHUTDOWN WAIT FOR PENDING HRECALL REQUESTS Can be set to the number of seconds the product's main task should suspend if outstanding DFHSM HRECALL requests are still outstanding. Shutdown is delayed while waiting for DFHSM to post outstanding requests completed. If set to zero, or if the **DFHSMSTATUS** parameter is set to 0FFLINE, no HRECALL completion handling is performed during shutdown.	0	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
DFHSMSTATUS	DFHSM SERVICES ARE OFFLINE/ONLINE Can be manually set during normal Server operations to temporarily suspend all Server interactions with DFHSM. The Server continues to remember all pending HRECALL requests and attempts to complete them and free the associated MWE blocks once this parameter is restored to DFHSMSTATUS(ONLINE). Administrators can use this option to temporarily suspend DFHSM processing during times when DFHSM services are unavailable, or DFHSM is being restarted. **Note:** When this parameter is manually altered, the **DFHSMDRAIN** parameter is automatically reset to `DFHSMDRAIN(NO)`.	ONLINE	Yes	No
FILEAPIRECALL	SWSFILE RECALL PROCESSING Determines whether data set recall is used when processing SWSFILE application programming interface requests. The parameter applies only to those requests which specify a DSNAME explicitly and only when the data set is not shared (i.e. Defined during startup). If set to AUTO, the values specified for the **FILERECALL**, **FILEHRECALL**, and **HRECALLWAIT** parameters are used. This option is strongly recommended for new customers. If set to ALLOCATE, data set recall for SWSFILE is handled by dynamic allocation processing. Existing customers may wish to set this option to maintain operational compatibility with previous releases of the product. If set to FAIL, data set migration is not allowed and the SWSFILE request fails when data set migration is required.	AUTO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
FILECACHE	DYNAMIC FILE CACHE OPTION Determines whether to cache PDS(E) and QSAM data sets that are being globally shared throughout the server. This option is applied only to those data sets which are made globally shared AFTER STARTUP. (This occurs when the FILESHAREDDN or FILESHAREDSN option is YES the first time an eligible /*FILE rule is executed; i.e. only for data sets which dynamically are made globally shared; not for data sets made shared using the DEFINE FILE start-up statement.) • ALL indicates that both data and PDS(E) directories should be cached for globally shared data sets. • NONE indicates that no caching is performed for these shared data sets. • DIR indicates that only PDS(E) directory entries are to be cached for shared data sets.	ALL	Yes	No
FILECLOSEAFTER	QUIESCE FILE AFTER TIME LIMIT Determines how long, in seconds, any PDS(E) and QSAM data sets that are being globally shared throughout the server remain open if they are not accessed. After expiration of this time, inactive data sets are closed and cached storage is released. This option applies only to those data sets made globally shared after startup. (This occurs when the FILESHAREDDN or FILESHAREDSN option is YES the first time an eligible /*FILE rule is executed; i.e. only for data sets which dynamically are made globally shared; not for data sets made shared using the DEFINE FILE start-up statement.) The allowable range is 0 to 32767 seconds. A setting of zero (0) indicates that there is no inactivity time limit and the data set remains open until the Server is shut down.	5	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
FILEHRECALL	DYNALLOC-TO-DFHSM RECALL CONVERSION Determines whether to internally convert dynamic allocation data set recall requests to asynchronous DFHSM HRECALL operations. Conversion of these requests can prevent system hangs upon the SYSZTIOT resource. When the DYNALLOC SVC handles data set recalls internally, long-term enqueues can be generated upon SYSZTIOT if a migrated data set cannot be recalled quickly. All other DYNALLOC requests stack up behind this enqueue. This parameter is ignored if DFHSM support is not enabled or is currently suspended. This parameter controls recall operations when data set allocation is performed for the following Server API interfaces: • SWSALLOC operations operating with RECALL(YES) specified, or using system-wide default action of FILERECALL(YES). • SWSFILE operations against a non-shared, DSNAME-based requests when FILEAPIRECALL(DEFAULT) is in effect. • WWW rule process sections, such as /*FILE, /*EXECSQL, /*EXECIMS, and so on. while processing a non-shared, DSNAME-based MVS data set when FILERULERECALL(DEFAULT) is in effect. The default setting is ALLOCATE, which indicates that DYNALLOC-to-DFHSM recall conversion is not performed. When data set recall is necessary (and allowed), the DYNALLOC SVC handles data set in-migration.	ALLOCATE	Yes	No
FILEMESSAGES	CONSOLE MESSAGES FROM DYNAMIC ALLOCATION Determines whether to allow a dynamic allocation error messages to be displayed upon the system console. This parameter only affects dynamic allocation requests made through the SWSALLOC application programming interface. The default setting is to allow error messages to be displayed upon the system console is YES.	YES	Yes	No
FILEMOUNT	MOUNT VOLUMES FOR DYNAMIC ALLOCATION	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
FILERECALL	RECALL FILES FOR DYNAMIC ALLOCATION Determines whether to allow a data set to be recalled to satisfy dynamic allocation requests. This parameter affects only dynamic allocation request made using the SWSALLOC application programming interface. Valid values are YES, NO, and NEVER. If set to YES, data set recalls can occur, but individual SWSALLOC requests can override using the RECALL() keyword. If set to NO, in-migration is not requested automatically and SWSALLOC request must specify RECALL(YES) if recall is to be allowed. If set to NEVER, data set migration is always suppressed for dynamic allocation requests and this setting cannot be altered using the RECALL() SWSALLOC keyword. Note that how data set recalls are performed internally is further controlled by the **FILEHRECALL** parameter. This parameter indicates only the default recall, no-recall, or never-recall defaults for the SWSALLOC API interface.	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
FILEREXXTOOLRECALL	FILE REXXTOOL RECALL PROCESSING Determines whether data set recall is used when processing Data Virtualization/ REXXTools dynamic allocation requests. It specifies how migrated data sets are handled when dynamic allocation is requested. Valid values are AUTO, ALLOCATE, and FAIL. If set to AUTO, recall processing is handled as specified by the **FILEHRECALL**, and **HRECALLWAIT** parameters. Use of this option is recommended for all new customers. If set to ALLOCATE, data set in-migration for requests are handled by dynamic allocation processing. Existing customers may wish to set this option to maintain operational compatibility with previous release of the product (this allows for no time out on recall requests, and may lead to hangs in SVC99 upon the SYSZTIOT queue name). If set to FAIL, data set recall is not allowed and if a migrated data set is requested, the dynamic allocation request fails.	AUTO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
FILERULERECALL	FILE RULE RECALL PROCESSING Determines whether data set recall is used when processing /*FILE rules, or to any other WWW rule process section which processes files as part of its operation (for example, the input/output forms used by /*EXECSQL sections). It specifically applies only to those rules which specify a DSNAME explicitly, and only when the data set is not shared (i.e. Defined during start-up). Valid values are AUTO, ALLOCATE, and FAIL. If set to AUTO, recall processing is handled as specified by the **FILEHRECALL**, and **HRECALLWAIT** parameters. Use of this option is recommended for all new customers. If set to ALLOCATE, data set in-migration for rules is handled by dynamic allocation processing. Existing customers may wish to set this option to maintain operational compatibility with previous release of the product (this allows for no time out on recalls requests, but may lead to hangs in SVC99 upon the SYSZTIOT queue name). If set to FAIL, data set recall is not allowed and if a migrated data set is requested, the rule operation fails.	AUTO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
FILESECURITY	DYNAMIC FILE SECURITY OPTION Determines who is authorized to read/ access PDS(E) and QSAM data sets that are being globally shared throughout the server. This option is applied only to those data sets which are made globally shared AFTER STARTUP. (This occurs when the FILESHAREDDN or FILESHAREDSN option is YES the first time an eligible /*FILE rule is executed; i.e. only for data sets which dynamically are made globally shared; not for data sets made shared using the DEFINE FILE start-up statement.) If set to SUBSYS, data sets which are made globally shared are accessed using the Server's userid for all authorization processing. Files/Members are served by WWW transactions without checking the TRANSACTION's effective userid for authorization to read the underlying data set. If set to USERID, data sets which are made globally shared are brought online and accessed using the Server's userid for authorization. Files/Members are, however, only served by WWW transactions if the TRANSACTION's effective userid has READ authorization to the data set. If the TRANSACTION's userid does not have sufficient authorization the data is not served, even though the Server can and does access the underlying data set.	SYBSYS	Yes	No
FILESHAREDDN	DEFINE NEW DDNAMES DYNAMICALLY Allows the user to control whether to share DDNames when possible. If a DDName is already open due to a previous allocation, this parameter controls whether the DDName can be accessed by multiple users or if the data set must be re-allocated to another DDName for a subsequent user. Valid values are YES (Share the DDName) or NO (Do not share the DDName).	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
FILESHAREDSN	DEFINE NEW DSNAMES DYNAMICALLY Determines whether data sets referred to by DS name in /*FILE rules are made globally shared by the Server. The parameter controls whether the data set can be accessed by multiple users or if the data set must be re-allocated to another DDName for a subsequent user. Valid values are YES (Share the data set) and NO (Do not share the data set).	NO	Yes	No
FILESTAGINGSIZELIMIT	FILE STAGING SIZE LIMIT When data files are processed for transmission by the server, all native MVS files must be pre-staged before actual outbound transmission can be performed. This is done to correctly calculate the outbound HTTP Content-length header, and to process HTML extension statements in the source text. Set this limit to specify a maximum file size for pre-staging data. The minimum size allowed is 64 KB (65536). This limit protects the system from overcommitting processor virtual storage while handling any single file service request. If the limit value is not an exact multiple of 64 KB, it is rounded to the next higher multiple. The maximum allowable limit size is 16 MB minus one. For files which exceed this limit, the Server aborts the processing of HTML extension statements and signals an oversize file condition. If possible, the original file request is re-driven using an alternate runtime processing algorithm. The alternate procedure re-opens the data set using a thread-owned DCB (to avoid holding a shared file for a long period of time). It then reads and transmits the file data to the client in 64 KB segments, up to the limit imposed by the **MAXHTTPRESPBYTES**. The server does not attempt to re-drive oversize file requests if they were originally requested by a REXX caller using DD name. This is because often REXX file allocations are temporary and freed at close, therefore, the file cannot be re-opened. Also, re-drive requests are honored only for SEND-to-client operations, and cannot be handled if HTML extension statements are present in the input data.	2097152	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
GDGLOCS	GDG LOCATE CATALOG SEARCH Allows the user to control how GDG relative generation numbers are located. GDG information is either based upon the GDG status the first time the product dynamically allocates a GDG data set, or the catalog is searched each time the data set is allocated. The default is GDG information is based upon the GDG status the first time the product allocates the file.	NO	Yes	No
HRECALLWAIT	WAIT TIME LIMIT FOR HRECALL Determines how long (in seconds) the server suspends task execution to await recall completion when DFHSM HRECALL is used for data set in-migration. If set to 0 (zero), HRECALL requests are issued without waiting on completion. Data set recall is scheduled using DFHSM, but the Data Virtualization Server does not wait on completion. The data set access operation fails and must be retried later. Note that in this case, the Data Virtualization Server does not track HRECALL requests in any way. Any positive number in the range 1 to 32767 determines the number of seconds to await recall completion. If HRECALL does not complete in the allotted time, the original request fails and must be retried.	45	Yes	No
HRECALLWAITMAX	MAX HRECALL WAIT TIME FOR SWSALLOC When DFHSM HRECALL is used for data set in-migration, this parameter determines the maximum HRECALL wait time that can be specified explicitly by an SWSALLOC application programming interface request using the RECALLWAIT() keyword. If an individual SWSALLOC request attempts to specify a longer wait time limit than is imposed by this parameter, the value specified by this parameter is substituted. See HRECALLWAIT for a description of the HRECALL wait time limits. The maximum value allowed for this parameter is 32,767 seconds.	45 SECONDS	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
MONRESPONSETIME	Monitor response time from client Monitors the client response time if application names have been defined in the IN00 start up exec using the DEFINE RTMONAPP statement if this parameter is set to *YES*.		YES	NO

PRODFILE parameter group

Parameter Name	Parameter description	Default value	Update	Output only
VSAMOPENRLS	DMF SHARE VSAM ACBS Controls if VSAM files should be shared among all tasks. The files are kept open unless VSAMRLSQUIESCE is also set.		NO	NO
VSAMRLSQUIESCE	DMF SHARE VSAM ACBS QUIESCE WHEN INACTIVE Causes shared VSAM files to be closed when the open use count is zero.		YES	NO
VSAMCONTROLFILE	DMF VSAM CONTROL FILE NAME Specifies the data set name of the control file for VSAM files. This file is shared among all copies of the product in the Sysplex. If this parameter is enabled, VSAMCONTROLAIX parameter must also be specified.		NO	NO
VSAMCONTROLAIX	DMF VSAM CONTROL FILE AIX Specifies the path name of the control file for VSAM files. This file is shared among all copies of the product in the Sysplex. This parameter must be enabled if the VSAMCONTROLFILE parameter is specified.		NO	NO

PRODGLV parameter group

Parameter name	Parameter description	Default value	Update	Ouput only
GLOBALALLOC	NUMBER OF ALLOCATED GLOBAL VARIABLE BLOCKS	3	No	Yes
GLOBALBACKUPCOUNT	GLOBAL VARIABLE BACKUP COUNT	0	No	Yes
GLOBALBACKUPEND	GLOBAL LAST BACKUP END TIME	NONE	No	Yes

Parameter name	Parameter description	Default value	Update	Ouput only
GLOBALBACKUPINTVAL	INTERVAL BETWEEN GLOBAL VARIABLE BACKUPS	0 MINUTES	Yes	No
GLOBALBACKUPNEXT	GLOBAL BACKUP NEXT START TIME	NONE	No	Yes
GLOBALBACKUPPROC	GLOBAL VARIABLE BACKUP PROC NAME	'00000000'	Yes	No
GLOBALBACKUPSTART	GLOBAL LAST BACKUP START TIME	NONE	No	Yes
GLOBALBLOCKS	GLOBAL CHECKPOINT BLOCK COUNT	626 PAGES	No	Yes
GLOBALBLOCKSUSED	NUMBER OF GLOBAL VARIABLE BLOCKS IN USE	3	No	Yes
GLOBALCHECKCOUNT	GLOBAL CHECKPOINT COUNT	2 CHECK-POINT	No	Yes
GLOBALDATE	GLOBAL LAST CHECKPOINT DATE	YYYY/MM/DD	No	Yes
GLOBALDIV	GLOBAL VARIABLES SHOULD USE DIV	YES	No	No
GLOBALFREE	NUMBER OF FREE GLOBAL VARIABLE BLOCKS	0	No	Yes
GLOBALFREEAREAS	NUMBER OF FREE AREAS IN GLOBAL WORKSPACE	0	No	Yes
GLOBALINTERVAL	GLOBAL VARIABLES CHECKPOINT INTERVAL	15 SECONDS	Yes	No
GLOBALLENGTH	GLOBAL WORKSPACE BLOCK LENGTH	256 BYTES	No	Yes
GLOBALMAX	MAXIMUM NUMBER OF GLOBAL VARIABLES	5000	No	No
GLOBALMSGS	GLOBAL ERROR MESSAGE COUNT	0	No	Yes
GLOBALNEXT	GLOBAL WORKSPACE NEXT FREE OFFSET	X'00000000'	No	Yes
GLOBALPAGES	GLOBAL WORKSPACE AREA SIZE IN PAGES	313 PAGES	No	Yes
GLOBALPOOL	GLOBAL WORKSPACE FREE POOL OFFSET	X'00000000'	No	Yes
GLOBALREBUILD	REBUILD GLOBAL VARIABLE DATABASE	None	Yes	No
GLOBALRETRY	GLOBAL CHECKPOINT RETRY COUNT	0 CHECK POINTS	No	Yes
GLOBALSIZE	GLOBAL WORKSPACE BLOCK SIZE	1250K	No	Yes

Parameter name	Parameter description	Default value	Update	Ouput only
GLOBALSUBPOOL	GLOBAL VARIABLES SUBPOOL NUMBER	TWO	No	No
GLOBALTCB	GLOBAL WORKSPACE TCB ADDRESS	X'00000000'	No	Yes
GLOBALTEMPUPDATE	TEMP GLOBAL VARIABLES UPDATE COUNT		NO	YES
GLOBALTEMPADDR	TEMPORARY GLOBAL WORKSPACE BLOCK ADDRESS	X'00000000'	No	Yes
GLOBALTEMPMAX	MAXIMUM NUMBER OF TEMPORARY GLOBAL VARIABLES	5000	No	No
GLOBALTEMPWARNIV	INTERVAL BETWEEN TEMP GLV BLOCKS USED WARNINGS	5 MINUTES	Yes	No
GLOBALTEMPWARNTH	TEMP GLOBAL BLOCKS USED WARNING THRESHOLD	80%	Yes	No
GLOBALTIME	GLOBAL LAST CHECKPOINT TIME	HH:MM:SS	No	Yes
GLOBALTOKEN	GLOBAL WORKSPACE TOKEN ID	X‘00000000000 0000000’	No	Yes
GLOBALUPDATE	GLOBAL VARIABLES UPDATE COUNT	1	No	Yes
GLOBALUPDATECOUNT	GLOBAL CHECKPOINT UPDATE COUNT	1	No	Yes
GLOBALUSED	NUMBER OF GLOBAL VARIABLES IN USE	3	No	Yes
GLOBALWARNINTVAL	INTERVAL BETWEEN GLOBAL BLOCKS USED WARNINGS	5 MINUTES	Yes	No
GLOBALWARNTHRESH	GLOBAL BLOCKS USED WARNING THRESHOLD	80%	Yes	No
GLVCHAINMAX	MAXIMUM NUMBER OF CHAINED GLV UPDATES	1000	Yes	No
GLVPENDINGMAX	MAXIMUM NUMBER OF PENDING GLV EPROCS	100	No	No
GLVSHAREDFILE	SHARED VARIABLE VSAM DATASET NAME		Yes	No

PRODHTML parameter group

Parameter name	Parameter description	Default value	Update	Output only
DEFAULTEXCIFORMURL	CICS/EXCI HTML DEFAULT FORM URL Specifies a default FORM URL to be used during the generation of HTML through the Data Virtualization Server Mapping Facility. This form is used to process the data on the HTML form. This parameter controls only HTML generated through the EXCI HTML generation option.	/SHDW/ EXCINTRY	Yes	No
DEFAULTGENFORMURL	GENERIC HTML DEFAULT FORM URL Specifies a default FORM URL to be used during the generation of HTML through the Data Virtualization Server Mapping Facility. This form is used to process the data on the HTML form. This parameter controls only HTML generated through the GEN HTML generation option.	<%WWW.CURR ENTURL%>	Yes	No
DEFAULTIMSFORMURL	IMS HTML default FORM URL Specifies a default FORM URL to be used during the generation of HTML through the Server Mapping Facility. This parameter is used to process the data on the HTML form and controls only the HTML file generated through the IMS HTML generation option.	/SHDW/ IMSENTRY	YES	NO
GENERATEFONTORDERS	Generate HTML Font Color orders. Specifies to generate a HTML FONT color order when generating a HTML file and the color of the text or data is decided. This parameter is used when generating IMS HTML for MFS source extracted through the server mapping facility.	YES	YES	NO

Parameter name	Parameter description	Default value	Update	Output only
GENERATESTYLECOLOR	Generate STYLE colors for input fields Specifies to generate a corresponding HTML FONT color order when generating a HTML file with and the color of the text or data is decided. This parameter is used when generating IMS HTML for MFS source extracted through the server mapping facility.	YES	YES	NO
ENCRYPTHIDDENDATA	Encrypt Auto-HTML hidden field data values Specifies to encrypt the value of HTML hidden fields when generating the fields. The server prefixes the field names with a special value and decrypts these values when they receive on any subsequent inbound request. This option applies only when generating and processing IMS HTML from MFS source extracted through the server mapping facility. The maximum size hidden field which can be encrypted is 512 bytes.	NO	YES	NO
HTMLFONTTURQUOISE	Replace TURQUOISE with this color Specifies the HTML color that is to replace 3270 display station TURQUOISE. This is generally used to translate IMS Extended Attribute colors.		YES	NO
HTMLBACKGROUNDCOLOR	HTML default background color Specifies a default font color when generating HTML using the Data Virtualization Server Mapping Facility.	000000 (Black)	Yes	No
HTMLDEFAULTFONTCOLOR	HTML default font color Specifies a default font color when generating HTML using the Data Virtualization Server Mapping Facility.	00F500 (Green)	Yes	No
HTMLFONTBLUE	Replace BLUE with this color Specifies the HTML color that is to replace 3270 display station BLUE. This is generally used to translate IMS Extended Attribute colors.	0000F5 (Blue)	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
HTMLFONTGREEN	Replace GREEN with this color Specifies the HTML color that is to replace 3270 display station GREEN. This is generally used to translate IMS Extended Attribute colors.	00F500 (Green)	Yes	No
HTMLFONTHILIGHT	Replace HILIGHT fields with this color Specifies the HTML color that is to replace highlighted fields on a 3270 display station. This value is generally used to translate IMS dynamic attributes.	FFFFFF (White)	Yes	No
HTMLFONTPINK	Replace PINK with this color Specifies the HTML color that is to replace 3270 display station PINK. This is generally used to translate IMS Extended Attribute colors.	FF6EC7 (Pink)	Yes	No
HTMLFONTRED	Replace RED with this color Specifies the HTML color that is to replace 3270 display station RED. This is generally used to translate IMS Extended Attribute colors.	F50000 (Red)	Yes	No
HTMLFONTWHITE	Replace WHITE with this color Specifies the HTML color that is to replace 3270 display station WHITE. This is generally used to translate IMS Extended Attribute colors.	FFFFFF (White)	Yes	No
HTMLFONTYELLOW	Replace YELLOW with this color Specifies the HTML color that is to replace 3270 display station YELLOW. This is generally used to translate IMS Extended Attribute colors.	FFFF00 (Yellow)	Yes	No
HTMLINPUTHILIGHT	Replace HILIGHT input font with this color Specifies the HTML color that is to replace highlighted font input fields on a 3270 display station. Input fields on a Web Browser have a white background. This value is generally used to translate IMS dynamic attributes.	F50000 (Red)	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
HTMLINPUTWHITE	Replace WHITE input font with this color Specifies the HTML color that is to replace white font input fields on a 3270 display station. Input fields on a Web Browser have a white background. This value is generally used to translate IMS dynamic attributes.	F50000 (Red)	Yes	No

PRODIDF parameter group

Parameter name	Parameter description	Default value	Update	Output only
IDF	ENABLE IDF DRDA SERVER Setting this parameter will activate and initialize the Integrated DRDA Facility (IDF) DRDA Application Server.		NO	NO
IDFLOCATION	IDF LOCATION NAME Provides the DRDA Application Server location name used by an IDF instance. The name must be unique across all connected systems and must be set prior to startup. The default value is the IDF server SubSystem ID concatenated behind the SMF ID to form an 8-byte name.		NO	NO
IDFOVERRIDECCSID	IDF OVERRIDES SQL ENGINE CCSIDS Causes IDF-specific CCSIDs to be used for DRDA TYPDEFOVR processing instead of the CCSIDs in use by the internal SQL Engine.		YES	NO
IDFCCSIDSBCS	IDF CCSID FOR SBCS Sets the IDF App-Server native SBCS character CCSID.		NO	NO
IDFCCSIDMBCS	IDF CCSID FOR MBCS Sets the IDF App-Server native MBCS character CCSID.		NO	NO
IDFCCSIDDBCS	IDF CCSID FOR DBCS Sets the IDF App-Server native BBCS character CCSID.		NO	NO
IDFDRBUPARSERSIZE	IDF DRBU PARSER SIZE Specifies the buffer parser area size in kilobytes. The minimum value that can be set is 256, and the maximum value that can be set is 960.		YES	NO

PRODIMS parameter group

Parameter name	Parameter description	Default value	Update	Output only
IMSDIRECTENABLED	IMS-DIRECT MAP REDUCE PROCESSING ENABLED Enables the usage of IMS-Direct map reduce processing.		YES	NO
IMSDIRECTMRDEFAULT	IMS-DIRECT MAP REDUCE TASK COUNT DEFAULT Specifies the default number of map reduce tasks to be attached for IMS-Direct processing. The default is used if the DBD data map contains no override value. The minimum value that can be set is 1 and the maximum value that can be set is 8.		YES	NO
IMSDIRECTCYLBUF	IMS-DIRECT BUFFER CYLINDER COUNT Specifies the number of cylinders of data to buffer for each file processed in an IMS-Direct task. The minimum value that can be set is 1 and the maximum value that can be set is 50.		YES	NO
IMSDIRECTMINTASKS	IMS-DIRECT MINIMUM TASKS Specifies the number of ACI tasks to keep active for IMS-Direct requests. The minimum value that can be set is 2 and the maximum value that can be set is 100.		YES	NO
IMSDIRECTOSAMRECSRD	IMS-DIRECT OSAM RECORDS PER READ Specifies the number of records to read in each OSAM I/O operation. The minimum value that can be set is 1 and the maximum value that can be set is 50.		YES	NO
IMSDIRECTBUFFERSIZE	IMS-DIRECT MAP REDUCE READ-AHEAD BUFFER SIZE Specifies the size of each read-ahead buffer used to collect IMS segments from map reduce threads for return to the SQL Engine task. The number is expressed in Kilobytes per buffer. Note that this size must be large enough to contain the largest possible IMS database record. The minimum value that can be set is 64KB and the maximum value that can be set is 2097152 KB.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
IMSDIRECTBUFFERCOUNT	IMS-DIRECT MAP REDUCE READ-AHEAD BUFFER COUNT Specifies the number of read-ahead buffers to be used for each map reduce thread. The minimum value that can be set is 2 and the maximum value that can be set is 10.		YES	NO
IMSDIRCMPXITSRB1	IMS-DIRECT SRB SAFE COMPEXIT 1 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRCMPXITSRB2	IMS-DIRECT SRB SAFE COMPEXIT 2 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRCMPXITSRB3	IMS-DIRECT SRB SAFE COMPEXIT 3 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRCMPXITSRB4	IMS-DIRECT SRB SAFE COMPEXIT 4 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRCMPXITSRB5	IMS-DIRECT SRB SAFE COMPEXIT 5 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRCMPXITSRB6	IMS-DIRECT SRB SAFE COMPEXIT 6 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
IMSDIRCMPXITSRB7	IMS-DIRECT SRB SAFE COMPEXIT 7 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRCMPXITSRB8	IMS-DIRECT SRB SAFE COMPEXIT 8 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRCMPXITSRB9	IMS-DIRECT SRB SAFE COMPEXIT 9 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRCMPXITSRB10	IMS-DIRECT SRB SAFE COMPEXIT 10 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRCMPXITTCB1	IMS-DIRECT TCB SAFE COMPEXIT 1 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the TCB mode but with no serialization. This improves the performance.		YES	NO
IMSDIRCMPXITTCB2	IMS-DIRECT TCB SAFE COMPEXIT 2 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the TCB mode but with no serialization. This improves the performance.		YES	NO
IMSDIRCMPXITTCB3	IMS-DIRECT TCB SAFE COMPEXIT 3 Specifies the name of IMS segment edit/ compression routines that are safe to run directly in the TCB mode but with no serialization. This improves the performance.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
IMSDIRCMPXITTCB4	IMS-DIRECT TCB SAFE COMPEXIT 4 The IMSDIRCMPXITTCB4 parameter specifies the name of IMS segment edit/ compression routines that are safe to run directly, in TCB mode, but with no serialization. This will afford improved performance.		YES	NO
IMSDIRCMPXITTCB5	IMS-DIRECT TCB SAFE COMPEXIT 5 The IMSDIRCMPXITTCB5 parameter specifies the name of IMS segment edit/ compression routines that are safe to run directly, in TCB mode, but with no serialization. This will afford improved performance.		YES	NO
IMSDIRCMPXITTCB6	IMS-DIRECT TCB SAFE COMPEXIT 6 The IMSDIRCMPXITTCB6 parameter specifies the name of IMS segment edit/ compression routines that are safe to run directly, in TCB mode, but with no serialization. This will afford improved performance.		YES	NO
IMSDIRCMPXITTCB7	IMS-DIRECT TCB SAFE COMPEXIT 7 The IMSDIRCMPXITTCB7 parameter specifies the name of IMS segment edit/ compression routines that are safe to run directly, in TCB mode, but with no serialization. This will afford improved performance.		YES	NO
IMSDIRCMPXITTCB8	IMS-DIRECT TCB SAFE COMPEXIT 8 The IMSDIRCMPXITTCB8 parameter specifies the name of IMS segment edit/ compression routines that are safe to run directly, in TCB mode, but with no serialization. This will afford improved performance.		YES	NO
IMSDIRCMPXITTCB9	IMS-DIRECT TCB SAFE COMPEXIT 9 The IMSDIRCMPXITTCB9 parameter specifies the name of IMS segment edit/ compression routines that are safe to run directly, in TCB mode, but with no serialization. This will afford improved performance.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
IMSDIRCMPXITTCB10	IMS-DIRECT TCB SAFE COMPEXIT 10 The IMSDIRCMPXITTCB10 parameter specifies the name of IMS segment edit/ compression routines that are safe to run directly, in TCB mode, but with no serialization. This will afford improved performance.		YES	NO
IMSDIRDECXITSRB1	IMS-DIRECT SRB SAFE DEC EXIT 1 Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRB2	IMS-DIRECT SRB SAFE DEC EXIT 2 Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRB3	IMS-DIRECT SRB SAFE DEC EXIT 3 Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRB4	IMS-DIRECT SRB SAFE DEC EXIT 4 Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRB5	IMS-DIRECT SRB SAFE DEC EXIT 5 Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRB6	IMS-DIRECT SRB SAFE DEC EXIT 6 Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
IMSDIRDECXITSRB7	IMS-DIRECT SRB SAFE DEC EXIT 7 Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRB8	IMS-DIRECT SRB SAFE DEC EXIT 8 Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRB9	IMS-DIRECT SRB SAFE DEC EXIT 9 Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRBA	IMS-DIRECT SRB SAFE DEC EXIT A Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRBB	IMS-DIRECT SRB SAFE DEC EXIT B Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRBC	IMS-DIRECT SRB SAFE DEC EXIT C Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRBD	IMS-DIRECT SRB SAFE DEC EXIT D Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
IMSDIRDECXITSRBE	IMS-DIRECT SRB SAFE DEC EXIT E Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRBF	IMS-DIRECT SRB SAFE DEC EXIT F Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRBG	IMS-DIRECT SRB SAFE DEC EXIT G Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRBH	IMS-DIRECT SRB SAFE DEC EXIT H Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRBI	IMS-DIRECT SRB SAFE DEC EXIT I Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRBJ	IMS-DIRECT SRB SAFE DEC EXIT J Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO
IMSDIRDECXITSRBK	IMS-DIRECT SRB SAFE DEC EXIT K Specifies the name of IMS segment decryption routines that are safe to run directly in the SRB mode with no serialization. This improves the performance.		YES	NO

PRODSECURITY parameter group

Parameter name	Parameter description	Default value	Update	Output only
ALLOWUNPROT	ALLOW ACCESS TO UNPROTECTED RESOURCES Specifies how Data Virtualization will deal with unprotected resources. When set to NO, Data Virtualization will fail unprotected resources with a resource not defined to RACF message. When set to YES, Data Virtualization will allow access to unprotected resources.	NO	Yes	No
AUTOSUPPLYVOLSER	AUTOMATICALLY SUPPLY VOLSER FOR SDBECURE API If set to YES, this parameter causes the SDBECURE API routines to automatically retrieve and supply a VOLSER for data set authorization requests. This is done only when a VOLSER is not already supplied by the caller. Supplying a VOLSER on data set authorization checking requests prevents access to data sets which have a RACF discrete security profile. Without the VOLSER, RACF may indicate that authorization to a data set is allowed, even though a subsequent OPEN attempt may fail with ABEND S913. In the absence of a caller-provided VOLSER, the system supplies this information automatically. **Note:** The system never attempts to supply a VOLSER for API requests which are issued while running in a cross-memory environment. (Certain types of SEF ATH rules operate in cross-memory mode.) Also, the VOLSER is not supplied if the data set has been migrated to offline storage by DFHSM or other space management product.	YES	Yes	No
BYPASSSEF	BYPASS SEF FOR RECONNECT PROCESSING Controls whether SEF are invoked when a client reconnects to the Data Virtualization Server. This is a performance enhancement used to speed up processing when an ODBC client reconnects to the server. This is important if VCF is in use. This parameter cannot be changed after product initialization because of security restrictions.	NO	No	No
CENSORAPIDATAVALUES	CENSOR VARIOUS API DATA VALUES Indicates whether display of various API data is restricted to authorized users. If set to NO, display of the data is unrestricted.	NO	Yes	No
CENSORHTTPRESP	CENSOR HTTP RESPONSE OUTPUT Indicates whether display of out-bound response data are restricted to authorized users. If set to NO, display of the data is unrestricted.	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
CENSORSSLAPIDATAVALS	CENSOR SSL VARIOUS API DATA VALUES Indicates whether display of various API data for SSL sessions are restricted to authorized users. If set to NO, display of the data is unrestricted.	NO	Yes	No
CENSORSSLAUTHDATA	CENSOR SSL AUTHORIZATION HTTP HEADER DATA Indicates whether display of inbound authorization data for SSL sessions are restricted to authorized users. If set to NO, display of the data is unrestricted.	YES	Yes	No
CENSORSSLHTTPRESP	CENSOR SSL HTTP RESPONSE OUTPUT Indicates whether display of outbound response data for SSL sessions are restricted to authorized users. If set to NO, display of the data is unrestricted.	NO	Yes	No
CENSORSSLQUERYDATA	CENSOR SSL URL QUERY DATA Indicates whether display of inbound URL query data for SSL sessions are restricted to authorized users. If set to NO, display of the data is unrestricted.	NO	Yes	No
CENSORTRACEWRITES	CENSOR ALL TRACE WRITES If set to YES, all potentially sensitive data is censored from trace data before it is written. In this situation, it is impossible to review trace data and obtain sensitive data from it. It may also make problem determination more difficult, because all data may be censored from certain records.	YES	Yes	No
CENSORURLAUTHDATA	CENSOR AUTHORIZATION HTTP HEADER DATA Indicates whether display of in-bound authorization data are restricted to authorized users. If set to NO, display of the data is unrestricted.	YES	Yes	No
CENSORURLQUERYDATA	CENSOR URL QUERY DATA Indicates whether display of inbound URL query data are restricted to authorized users. If set to NO, display of the data is un-restricted.	NO	Yes	No
CENSORWSAUTHDATA	CENSOR WEB SERVICE AUTHORIZATION DATA Indicates whether display of in-bound Web Service authentication data are restricted to authorized users. If set to NO, display of the data is unrestricted.	NO	Yes	No
CLIENTLOGON	CLIENTS CAN BE AUTHENTICATED BY NOS	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
CLIENTLOGONLOGOPT	NORMAL CLIENT LOGON RACF LOG= OPTION If set to ASIS, normal client logon is issued with LOG=ASIS in effect. If set to ALL, then normal client logon is issued with LOG=ALL in effect. If set to NONE, then normal client logon is issued with LOG=NONE in effect. This option applies only to RACF systems and is also used for client logoff operations.	ASIS	Yes	No
CLIENTLOGONSTATOPT	NORMAL CLIENT LOGON RACF STAT= OPTION If set to ASIS, normal client logons are issued with STAT=ASIS in effect. If set to NO, then normal client logons are issued with STAT=NO in effect. This option applies only to RACF systems.	ASIS	Yes	No
DRIVERSYSPLEXAUTH	DRIVER SYSPLEX AUTHENTICATION Allows IOCTL access to collect USERID and UTOKEN information about driver connections when the driver and the server are executing in the same SYSPLEX environment. This will allow driver clients on the same SYSPLEX to choose to use the active z/OS authentication, by not providing the USERID and PASSWORD. When a USERID and a PASSWORD or other authentication are provided, the supplied credentials take priority over active client driver SYSPLEX authentication for the current TCP/IP connection.	NO	Yes	No
EXPIRESECOPTENTRIES	EXPIRE USER SECURITY CACHE ENTRIES Causes all SOM cache entries on this Data Virtualization Server to be marked expired. This produces a processing delay for the next remote support task that performs a logon or logoff.	NO	Yes	No
EXPOSEWWWPASSWORD	EXPOSE CLEAR-TEXT PASSWORD IN WWW.PASSWORD Controls whether client passwords provided by the HTTP request Authorization: header are instantiated in clear text form as the runtime variable WWW.PASSWORD. The default setting NO is recommended because otherwise, any Web transaction program has access to client passwords. **Note:** WWW.PASSWORD is built only across the password sent via browser userid/password prompting and is not set for any other passwords processed by the system	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
GETLOGONMESSAGES	GET ALL SAF LOGON MESSAGES Controls whether all of the messages from SAF LOGON processing should be obtained. If set to YES, all of the messages are obtained. Note that setting this parameter to YES forces the security control blocks to be located below the 16 MB line. If set to NO, only a subset of the SAF LOGON messages are obtained from the SAF interface; however, it is possible to locate the security control blocks above the 16 MB line.	NO	Yes	No
HEXIPSOURCE	USE HEXADECIMAL IP ADDRESS AS SOURCE Indicates that the SOURCE for SAF calls are set to the hexadecimal form of the IP address for clients connected using TCP/IP. This flag only applies to TCP/IP connections. The four-byte binary IP address is converted to an eight-byte upper case hexadecimal string. This string is used as the SOURCE for SAF calls. The SOURCE is where the SAF request is presumed to have come from. This used to mean terminal name and now has other meanings as well.	NO	No	No
HFSAUTHMODE	HFS AUTHORIZATION OPERATING MODE Determines how security authorization processing is performed when serving HFS-resident files. **HFSAUTHMODE(GLOBAL)** specifies that ALL accesses to any HFS-resident file or directory paths are made using the authorizations granted to the Server's default Runtime userid (the Userid specified by the **WWWDEFAULTRUNAUTH** parameter). The Server switches to this Userid before any access to an HFS-resident file is made and restores the pre-existing security environment after each access. **HFSAUTHMODE(THREAD)** specifies that all accesses to any HFS-resident file or directory paths are made using the authorizations granted to the transaction thread userid. **Note: HFSAUTHMODE(THREAD)** is the preferred operational mode, however, the default is **HFSAUTHMODE(GLOBAL)** to maintain compatibility with previous releases of the product.	GLOBAL	No	No

Parameter name	Parameter description	Default value	Update	Output only
IDFALREADYVERIFIED	IDF ALREADY-VERIFIED SECURITY REQUIRED Specifies the minimum authentication level that can be used when a client connects to the IDF DRDA Application Server. YES- Indicates that userid-only logons are supported with authentication already performed by the connecting DRDA client requestor. NO (DEFAULT VALUE) - Indicates that both a userid and a password or other supported authentication mechanism is required and will be verified by IDF.	No	Yes	No
JAVARESOURCETYPE	RESOURCE TYPE FOR JAVA Specifies the name of the security server's class (or resource type for ACF2) that is used to perform access authorization checks for BPEL resources.	NO	Yes	No
KERBEROSACTIVATE	KERBEROS FLAG ACTIVATE Activates the Kerberos Security API for the server. The default value is NO, and setting a value of YES will allow Kerberos secured object processing to occur. The Kerberos server DAEMON will be accessed to verify the Kerberos configuration. The Kerberos API LOAD module will be LOADED from the STEPLIB to perform initialization of the Kerberos API. Once all steps are completed, the active server will process Kerberos security requests. If the DAEMON is not active, the server will continue to attempt contact with the Kerberos server DAEMON on every secured object request until the Kerberos DAEMON becomes active. Kerberos Token or Ticket Object processing will not be available until the Kerberos DAEMON has fully initialized. All Kerberos secured object processing will fail with Security Errors until the value of KERBEROSAPIACTIVE is set to YES. In addition, other information Kerberos settings will not be updated until the Kerberos API is active and the configuration is verified. **Note:** If the server is active, this option should only be modified under direct supervision of a product support specialist. Use of the xVZyIN00 PARAM is the preferred method to modify the server PARAM. If the Kerberos API LOAD module cannot be LOADED, Kerberos support will be deactivated for the active Server execution, and KERBEROSACTIVATE will be reset to a value of NO.	No	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
KERBEROSACTIVATE	KERBEROS FLAG ACTIVATE Activates Kerberos Security API for the server. Setting this parameter allows Kerberos Secured Object processing to occur. The Kerberos Server DAEMON will be accessed to verify Kerberos configuration. The Kerberos API LOAD module will be loaded from STEPLIB to perform initialization of Kerberos API. Once the necessary steps are completed, the active server will process Kerberos security requests. If the DAEMON is not active, the server will continue to attempt to contact with the Kerberos Server DAEMON on every secured object request until the DAEMON becomes active. Kerberos Token or Ticket Object processing will not be available until the DAEMON is fully initialized. All Kerberos Secured Object processing will fail with security errors until the value of KERBEROSAPIACTIVE is set to *YES*. In addition, other information Kerberos settings will not be updated until the Kerberos API is active and the configuration is verified. Use the xVZyIN00 PARAM to modify this parameter. **Note:** This parameter should only be modified under direct supervision of a product support specialist, once the Server is active. If the Kerberos API LOAD module cannot be loaded, Kerberos support will be deactivated for active Server execution and KERBEROSACTIVATE parameter will be reset to a value of *NO*.	NO	YES	NO
KERBEROSAPIVERS	KERBEROS API VERSION/BUILD Specifies the Kerberos API Version/Build information collected after initialization of Kerberos API. This option is Server modified and informational only.		NO	YES
KERBEROSCLIENTONLY	IN-BOUND KERBEROS CLIENT ONLY Allows only Kerberos authentication when this parameter is set to *Yes*. If this parameter is set to *No*, the Server will allow both legacy z/OS USERID/PASSWORD authentication and Kerberos authentication. The value of *No* allows a transition from legacy z/OS USERID/PASSWORD authentication to Kerberos.		YES	NO
KERBEROSCLIENTS	KERBEROS IN-BOUND CLIENTS SUPPORTED Allows Kerberos authentication when the parameter is set to Yes. if the parameter is set to No, the server will not activate inbound Kerberos client authentication.		Yes	No

Parameter name	Parameter description	Default value	Update	Output only
KERBEROSCLIENTSPN	KERBEROS CLIENT SPN ALIAS This parameter is an optional parameter that needs the supplied SPN Alias be defined in the Kerberos DAEMON configuration. If the SPN verification fails, Kerberos processing is halted. And the Kerberos ticket will not be available. KERBEROSFAILED value will bet set to YES. This option allows Kerberos to be revoked from a server process by removing the SPN. This option can be modified after server initialization. **Note:** Even after verification, a secondary verification will occur due to the fact that the Kerberos DAEMON requires a follow-up verification of the configuration. This secondary verification scenario occurs normally after a restart or any authentication time-out.		Yes	No
KERBEROSDAEMONSPN	KERBEROS DAEMON SPN ALIAS This optional parameter verifies the Kerberos DAEMON SPN Alias after the server verifies the DAEMON SPN against the value supplied. If the supplied Alias is valid, processing will continue. If the supplied Alias is invalid, Kerberos Security will be disabled and all Ticket/Token Object request will fail. The default value for this parameter is an empty string of blanks/nulls to allow the server to discover the DAEMON SPN value, provided that the optional value informs the Server to verify the DAEMON SPN Alias. **Note:** Modification to this parameter will not become active until the Kerberos DAEMON is refreshed or the DAEMON requests the active server security credentials to be re-verified.		Yes	No
KERBEROSDAEMONV	KERBEROS DAEMON VERSION / BUILD Enables collection of Kerberos DAEMON Version/ Build information from the DAEMON server during Kerberos configuration process.		No	Yes
KERBEROSDSCLIENT	TYPE(SERVER) OUT/IN BOUND KERBEROS If this parameter is set to YES, the Server will use Kerberos authentication while performing attach/ bind/logon authentication to TYPE(SERVER) with SECMEC(KERBEROS). The requesting server will send the Kerberos token to the target Server for authentication.		Yes	No

Parameter name	Parameter description	Default value	Update	Output only
KERBEROSECHOSPN	KERBEROS SERVER ECHO SPN 2 CLIENT When a client attempts to authentication with a SPN which is rejected by the Server: • Setting this parameter to YES will inform the server in an authentication failure message to ECHO the SPN. The client can then attempt to authenticate with the SPN value returned by the Server. • Setting this parameter to NOwill cause the server to reject the authentication and not to provide the SPN with the login failure message.		Yes	No
KERBEROSFAILED	KERBEROS FLAG FAILURE This option is set only when the KERBEROSACTIVATE parameter is set to YES and the configuration is invalid or the API LOAD module was not found in the STEPLIB. This parameter value is set to YES when the Kerberos API initialization is failed, and it remains NO until a failure occurs.		Yes	No
KERBEROSGRANDE	KERBEROS FLAG GRANDE This option is set to Yes when the KERBEROSACTIVATE is YES and the module defined in KERBEROSLOAD is defined as an AMODE64 module. This option remains as No when AMODE31 processing is assumed.		No	Yes
KERBEROSHOST	KERBEROS HOST IPADDRESS/DOMAIN Provides the host ip address/domain of Kerberos ticket server DAEMON. The default value of this parameter is 127.0.0.1.		No	No
KERBEROSLOAD	KERBEROS API LOAD MODULE NAME Provides the Kerberos API LOAD module name that processes Kerberos ticket object requests for the active server.		No	No
KERBEROSMAXTICKET	KERBEROS API MAX TICKET/TOKEN SIZE Specifies the maximum size of Kerberos ticket/ token objects. The value of the default maximum is 1024*2 or 2K. Setting the value may reduce storage requirements when Kerberos Ticket/Token Objects are much smaller than the system default			
KERBEROSPORT	KERBEROS DAEMON PORT NUMBER Provides the port number used to access the Kerberos ticket server DAEMON.	5628	NO	NO

Parameter name	Parameter description	Default value	Update	Output only
KERBEROSTIMEOUT	KERBEROS API TIME OUT Defines an override of the standard Kerberos API TCP/IP time out value. The default value of -1 indicates no override of API TCPIP timeout is required. Setting the value to 0 will negate timeout processing. The range of values for this parameter is from 0 to 120.	-1	YES	NO
KERBEROSTRACE	KERBEROS API TRACE VALUE Defines the type of traces Kerberos processing will create during execution of Kerberos requests. The default value of -1 indicates quiet tracing with 0 through 6 providing an increasing level of trace from 0 failures to 6 debug.	-1	YES	NO
PASSEMPTYGROUPNAME	PASS EMPTY GROUP NAME TO RACROUTE Specifies whether a SAF-based RACROUTE REQUEST=VERIFY call passes a NULL group name on the request. Passing a NULL group name allows a user-written SAF exit routine, such as ICHRTX00, to manipulate the group name, even though Data Virtualization does not furnish or otherwise process RACF-type group names.	NO	Yes	No
PASSIMSGROUPNAME	PASS SAF GROUP NAME TO IMS Specifies whether to pass the SAF group name to IMS. Passing the SAF group name in the **PROFILE** parameter allows the group name, associated with the USERID, to appear in the I/O PCB of the IMS transaction.	NO	Yes	No
PASSTICKETAPPNAME	APPLICATION NAME FOR PTKTDATA PROFILES Specifies the 1 to 8-character application name to be used in PTKTDATA profiles.	XDBY XXXX	No	No
PASSWORDCASE	USER PASSWORD CASE Specifies whether passwords are used exactly as received (ASIS) or should be translated to upper (UPPER) case.	UPPER	No	No

Parameter name	Parameter description	Default value	Update	Output only
PROVIDEPASSWORDS	PROVIDE PASSWORDS FOR LOGON RULES Controls whether passwords are provided to LOGON rules. If this parameter is set to YES, passwords are provided to LOGON rules. If set to NO, passwords are not provided to LOGON rules. If set to CHANGE, passwords can be changed in LOGON ATH rules. Changing a password in a LOGON ATH rule does not change the password in the security product. It only changes the password used for the current connection to the host. For security reasons, this parameter cannot be changed after product initialization. Note that passwords are provided as cleartext strings or they are set to blanks.	NO	No	No
PUBLISHJCADETAIL	PUBLISH J2CA DETAIL PROF Used when authorizing J2CA publishing of events. When set to YES, causes the use of detailed security profiles when authorizing a J2CA user to monitor changes to tables. Detailed profiles are of the form PUBLISHJ2CA.source.tablename.	NO	Yes	No
RACFGROUPLIST	CHECK RACF GROUP LIST FLAG	NO	Yes	No
RECONNLOGONLOGOPT	RECONN CLIENT LOGON RACF LOG= OPTION If set to ASIS, the VCF-reconnect logon is issued with LOG=ASIS in effect. If set to ALL, then VCF-reconnect logon is issued with LOG=ALL in effect. If the parameter is set to NONE, then reconnect client logon is issued with LOG=NONE in effect. This option applies only to RACF systems and is also used for client logoff operations.	ASIS	Yes	No
RECONNLOGONSTATOPT	RECONN CLIENT LOGON RACF STAT= OPTION If set to ASIS, the VCF-reconnect logons are issued with STAT=ASIS in effect. When set to NO, then VCF-reconnect logons are issued with STAT=NO in effect. This option applies only to RACF systems.	ASIS	Yes	No
RESOURCETYPE	RESOURCE TYPE FOR RESOURCE RULES	NON	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
RULESETSEFAUTH	RULESET SEFAUTH() OVERRIDE Indicates whether the SEFAUTH() settings for individual rulesets are honored or overridden on a global basis. If NOOVERRIDE is set, each individual ruleset's SEFAUTH() setting is honored. If NONE, READ, UPDATE, or ALL is set, all ruleset level SEFAUTH settings are ignored and this setting is used instead. The ruleset SEFAUTH() setting determines whether SEF directly checks each command request to see if the end user has MVS authorization to the underlying ruleset before performing an operation on behalf of the user. Examples of such operations are enabling a rule, setting a rule's auto-enable flag, or putting a ruleset in offline status. Note that this checking is in addition to checking the end user's authorization to use SEF facilities. The SEF facility check is always performed using the "SEF" resource in the Server's resource class list. SEFAUTH specifies the level of operation that does not require authorization to proceed. A lower level of SEFAUTH means that less control is exerted over the operations on rules.	NOOVERRIDE	Yes	No
RULESETSEFAUTH	In increasing magnitude of authorization required, the options are: • SEFAUTH(NONE) specifies that SEF never checks the end user's authorization for any operation. • SEFAUTH(UPDATE) specifies that SEF does not check authorization for read-only and single-member-update operations, such as enabling a rule or setting a rule's auto-enable flag. SEF checks the end user's authorization for mass member updates or for changing the status of an entire ruleset. • SEFAUTH(READ) specifies that SEF does not check the end user's authorization when performing a read-only operation such a displaying a ruleset member list or status of an individual rule. SEF checks the end user's authorization for single-member-update operations or for mass member updates. • SEFAUTH(ALL) specifies that SEF always checks the end user's authorization for each operation. Note that MVS always performs an authorization check if an end-user attempts to browse, edit or delete a ruleset member under ISPF. This option specifies only how requests are handled when they are processed in the SEF subtask inside the server on behalf of a user-originated command.	NOOVERRIDE	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
SECOPTRETAIN	SECURITY OPT RETENTION PERIOD Specifies the amount of time in seconds that a cached security environment (ACEE) is to remain valid. When the time limit is reached, the cached security environment is invalidated. A value of zero means that cache entries are retained indefinitely. The default value is 28800 seconds (8 hours). This option only has meaning when the **SECURITYOPTIMIZATION** option is set to YES.	28800	Yes	No
SECOPTTARGET	SECURITY OPT CACHE TARGET ENTRIES Specifies the target number of user security environments (ACEE) to keep in the user security cache. The value can be from 500 to 100,000. Note that this target number increases if there are not enough available cache entries to maintain an entry for all currently logged on users. This option only has meaning when the **SECURITYOPTIMIZATION** option is set to YES.	5000	No	No
SECOPTTHRESHINT	SECURITY OPT THRESHOLD CHECKING INTERVAL Specifies the interval, in seconds, that SOM cache is scanned to find entries eligible for deletion from the cache. The interval value is specified in seconds and should be a factor of one hour. In other words the value should divide evenly into 3600. This option only has meaning when the **SECURITYOPTIMIZATION** option is set to YES.	1200	Yes	No
SECOPTTHRESHOLD	SECURITY OPT THRESHOLD VALUE Specifies the target number of SOM cache entries that are to be made available by SOM threshold interval processing, expressed as a percentage of the current number of allocated cache entries. The value can be from 5 to 100 percent. The default value is 25 percent. Specifying a small percent saves CPU time, but increases the number of expired, unused ACEEs that are kept in storage. Specifying a larger percent will reduce the number of expired and unused ACEEs kept in storage.	25	Yes	No
SECURITYMODE	SHARED SECURITY MODE Controls how security environments are shared. If this parameter is set to NONE, then security environments cannot be shared. If this parameter is set to BASIC, then some sharing of security environments is possible. This field cannot be changed after product initialization because of security restrictions. The server ignores this parameter when SOM is active (**SECURITYOPTIMIZATION** is set to YES).	NONE	No	No

Parameter name	Parameter description	Default value	Update	Output only
SECURITYMSGSUPP	SUPPRESS MESSAGES FROM RESOURCE CHECKS If set to YES, the product issues RACF security resource check requests with MSGSUPP=YES specified. If resource validation fails, a TSO user is not notified of the authorization failure.	NO	Yes	No
SECURITYOPTIMIZATION	SECURITY OPTIMIZATION ENABLED Specifies whether Data Virtualization caches the security environments (ACEE) created for successful remote user logons.	YES	No	No
SECURITYPACKAGE	SECURITY PRODUCT	RACF (depending on Security product)	No	Yes
SECURITYVERSION	SECURITY PRODUCT VERSION	7.74 (depending on Security product)	No	Yes
SQLVTRESOURCETYPE	RESOURCE TYPE FOR SQL ACCESS TO VIRTUAL TABLES Contains the name of the security server's class (or resource type for ACF2) that is used to perform authorization checks for SQL access to meta data and virtual tables in the SQL engine.		YES	NO
SSL	SSL CONNECTIONS SUPPORTED If set to YES, SSL connections to the server are supported. If set to NO, SSL sessions are not supported.	YES	No	No
SSLAUTODETECT	AUTO-DETECT SSL CONNECTIONS If set to YES, the server auto-detects SSL connections which are sent on the port normally used for clear-text connections. If this option is set to NO, only cleartext connections can be handled on the cleartext port. **Note:** A separately configured SSL port accepts only SSL connections.	NO	No	No

Parameter name	Parameter description	Default value	Update	Output only
SSLCLIENTAUTH	SSL CLIENT AUTHENTICATION The SSLCLIENTAUTH parameter activates optional SSL Client certificate processing in the Server, and also selects the means by which SSL Client certificates are authenticated when received. The values valid for this parameter are: • NONE: The Server does not make SSL client certificate processing active and will not request client certificates. This is the default setting. • LOCAL: The Server requests a client certificate during the SSL connection setup handshake. Certificates sent by the client are authenticated using the certificate store designated by other SSL startup parameters: Either a GSK SSL key database, or a RACF keyring. • PASSTHRU: The Server requests a client certificate during the SSL connection setup handshake. Certificates sent by the client are not authenticated upon receipt but are available for inspection by the transaction. Configuration of SSL support for use in Data Virtualization Server requires that you designate the location of the certificate and key store that the IBM-supplied SSL components will use. The server's SSL support may be configured to use a pair of “native” IBM SSL key database and key stash files. These files are maintained by the GSKKYMAN utility; a part of the IBM System SSL component. Alternatively, SSL may be configured to rely upon RACF (or SAF) digital certificate support which utilizes a designated RACF keyring as the store for the information. The designation of a certificate/key store, and the active content of the store have special impacts upon client certificate processing; impacts not always discussed nor easily located in the available documentation	NONE	No	No

Parameter name	Parameter description	Default value	Update	Output only
SSLCLIENTAUTH	One important bearing this has upon client certificate handling is the number and type of certificates present in the SSL database or keyring. During SSL session setup, the Server requests that the client transmit its certificate, and sends a list of those issuing authorities it trusts as acceptable. This list is built from the trusted CA certificates found in the SSL database or RACF keyring. A client may possess a separate certificate issued and signed by each of the most secure and well-known CA signing authorities. However, if none of those CA certificates are defined as trusted within the active database or keyring, then none will be sent to the client as an acceptable signer. Such a scenario would result in a client finding no acceptable alternatives and failing to return any certificate. Be aware that client's may fail to transmit any certificate, precisely because the list of trusted signers, at the host, is incomplete or deliberately and selectively limited. The second impact that SSL key storage configuration values affect is the ability of the Server to “convert” a valid certificate into a client logon to the z/OS system. When a RACF keyring is used as the SSL database, client certificates may optionally be used to drive the Init_ACEE callable service. The service may be able, if properly configured, to “map” the certificate received to produce an associated RACF userid logon. “Conversion” of client digital certificates into a RACF client logon can only be done when the SSL configuration settings designate a RACF keyring for the SSL key store.	NONE	No	No

Parameter name	Parameter description	Default value	Update	Output only
SSLCLIENTNOCERT	ACTION IF SSL CLIENT PROVIDES NO CERTIFICATE This parameter is ignored unless SSL Client certificate processing is activated (**SSLCLIENTAUTH**). This parameter setting indicates the action to be taken if an SSL client fails to provide a valid x501 certificate during session establishment. Note that a Client's failure to provide a certificate may be due to the lack of mutually trusted signing authority. Lack of a certificate does not prevent the SSL session from being established and used. The following values can be coded, each designating the action taken if the condition occurs. **Note:** The SSL handshake at session establishment completes prior to application of the FAILURE action If set to ALLOW, the Server continues processing, ignoring the Client's failure or inability to provide a certificate. If set to FAIL, the Server terminates its session with the client at the earliest possible opportunity.	ALLOW	No	No
SSLINITIALIZED	SSL SUPPORT HAS BEEN INITIALIZED Displays YES if SSL support was initialized.	NO	No	Yes
SSLUSERID	SSL RESOURCE MANAGER TASK USERID Specifies a highly-privileged userid under which the SSL resource manager subtask operates. If not specified, the SSL resource manager operates using the subsystem's address-space-level userid. This userid must be authorized to open and read the SSL Private Key and Certificate files. Use of a separate userid for this task prevents other transaction subtasks, and prevents the server from accessing this highly confidential information.	NULL	No	No
STANDARDUSERID	DEFAULT RUNAUTH USERID Specifies the MVS userid under which all work is run. The userid specified is made the effective userid for Web transactions unless WWW rules override this value. If the parameter is set to NONE, then the subsystem’s userid is used.	NONE	No	No
STREAMSJCADETAIL	FORCE DETAILED PROFILES FOR J2CA Causes the usage of detailed security profiles while authorizing a J2CA user to monitor changes to tables. Detailed profiles are in the form PUBLISHJ2CA.source.tablename.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
TERMINATESECOPT	TERMINATE SECURITY OPTIMIZATION Causes SOM to terminate. If set to YES, SOM ends and cannot be restarted. This parameter can be set at any time. Terminating SOM has an impact on Data Virtualization and overall system performance.	NO	Yes	No
TLSDYNAMICUSERIDS	IMPLEMENT DYNAMIC USERIDS FOR TLS Controls whether the generic userids supplied by a TLS-enabled connection are made active prior to most operations in Data Virtualization. The SEF logon rule sets the TLS-enabled option and this option determines if the supplied generic userid is used for RPC invocations, DB2 threads (only for RRSAF), CICS transactions, and so on.	YES	No	No
UNCENSORZOOMONLY	UNCENSOR ZOOM VIEW ONLY If set to N0, unauthorized users' view of trace messages is censored. Authorized users see the view uncensored. If set to YES, both unauthorized and authorized user's view of the trace data appears censored; however, authorized users may still view the uncensored data by displaying the underlying binary information.	NO	Yes	No
URLRESOURCETYPE	RESOURCE TYPE FOR URL MATCHING	NON	Yes	No
USEPORTOFENTRY	USE REMOTE HOST NAME AS PORT OF ENTRY Indicates that the remote computer's host name is to be used as the port of entry for user authentication. The port of entry can be used to restrict the computers from which a user can connect.	YES	No	No
USERIDENCODEALLOW	USERID ALLOW DRIVER ENCODED Allows *USERID* provided by drivers to be ENCODED during authentication when this parameter is set to *YES*. When set to YES the Server will allow, but not require ENCODED USERID values. This setting provides the ability for new drivers to send USERID values that are ENCODED or Clear text, provides toleration for older Drivers which do not support encoded USERID.		YES	NO
USERIDENCODEREQUIRED	USERID REQUIRE DRIVER ENCODED Specifies that the *USERID* provided by drivers should be encoded during authentication when this parameter is set to *Yes*. For drivers that do not have encoding support, the corresponding *USERID* will not be allowed to authenticate. If older driver support is required, use USERIDENCODEALLOW. .		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
VCFMAXLIFETIME	SECURITY OPT VCID RETENTION LIMIT Client connections that request the use of Diffie-Hellman key exchange for encryption of logon credentials require an extra round trip during session establishment to exchange public keys. For clients using the PERMANENT connection mode, the overhead entailed by the extra round trip is usually negligible in comparison to the total number of round trips made throughout the session. For non-permanent connection mode (VCF TRANSBLOCK or TRANSACT mode), in which a new connection is established for each client request, the ratio of key exchange round trips is much higher; often as high as 50% of all network trips. To avoid extra round trips, VCF can cache Diffie-Hellman key exchange information during the initial connection and recall the information when each VCF reconnection occurs. For this, the server creates a cache VCF security artifact at the host. Note that VCF security artifacts are only used when clients request the use of Diffie-Hellman key exchange for encryption of logon credentials, and only for clients making non-PERMANENT (VCF) mode session connections. If set to 0, no VCF security artifacts are created and each VCF connection or reconnection makes the extra round trip needed for Diffie-Hellman key exchange. When this parameter is set to a non-zero value, VCF security artifacts are created at the host and used to avoid the extra round trip for key exchange. The server substitutes 60 seconds if the value specified is in the range from 1 to 59. A non-zero value specifies the total time, in seconds, that a cached VCF security artifact remains valid. VCF security artifacts are aged from the time they are created up to this limit, and are unconditionally expired once this period has ended. Unreferenced VCF artifacts may time out and be expired (see VCFTIMEOUT) sooner than the lifetime limit imposed by this parameter.	1800 SECONDS	No	No

Parameter name	Parameter description	Default value	Update	Output only
VCFTIMEOUT	SECURITY OPT VCID REUSE TIMEOUT PERIOD This parameter is not used when **VCFMAXLIFETIME** has been set to zero. See the explanation for the **VCFMAXLIFETIME** parameter for a description of VCF security artifacts. This parameter specifies, in seconds, the time period in which a VCF security artifact must be re-referenced to remain active. Any VCF artifact that goes unreferred to for longer than the time period specified is considered expired and are deleted. The time limit value specified for this parameter should not exceed the value set for the **VCFMAXLIFETIME** parameter. If an invalid value is specified, the server substitutes the same value set for **VCFMAXLIFETIME**.	300 SECONDS	No	No
WWWDEFAULTAUTHREQ	DEFAULT WWW RULE AUTHREQ VALUE Specifies the default WWW AUTHREQ value under which Web transactions run. The AUTHREQ specification can be overridden through matching to WWW rules.	NO	No	No
WWWDEFAULTRUNAUTH	DEFAULT WWW RULE RUNAUTH USERID Specifies the MVS user ID under which Web transactions, by default, run. The user ID specified is made the effective userid for Web transactions unless WWW rules override this value. If set to NONE, then the subsystem's user ID is used. The user ID must have the authority to logon to the server.	NONE	No	No
WWWRUNAUTHFORMATS	RUNAUTH OPERAND FORMATS Used to limit the allowed operand formats. If set to RESTRICTED, RUNAUTH cannot be used to specify third-party userids.	ALL	No	No
WWWRUNAUTHLOCATION	RUNAUTH ALLOWED LOCATION Specifies where the **RUNAUTH** parameter may be coded for /*WWW rules. It may be restricted to the master WWW ruleset only, or disabled using this parameter.	ANYWHERE	No	No
ZEVRESOURCETYPE	RESOURCE TYPE FOR Z/EVENTS Specifies the name of the security server's class (or resource type for ACF2) that is used to perform access authorization checks for z/Events resources.	NON	Yes	No

PRODTRACE parameter group

Parameter name	Parameter description	Default value	Update	Output only
ACIINTERNALTRACEIN	TRACE ACI INTERNAL INPUT BUFFER Traces the ACI INTERNAL task input buffers at execution time into the Server Trace.	No	Yes	No
ACIINTERNALTRACEOUT	TRACE ACI INTERNAL OUTPUT BUFFER Traces the ACI INTERNAL task output buffers at execution time into the Server Trace.	No	Yes	No
ACITRACE	TRACE ACI EVENTS Specifies whether to trace ACI events.	NO	Yes	No
ACITRACEFULL	TRACE FULL ACI BUFFERS Traces the ACI output buffers at execution time into the Server Trace	No	Yes	No
ACITRACEGETBUF	TRACE ACI GET / FREE CALLS Controls tracing of ACI buffer pool get and free requests.			
ACITRACEIN	TRACE ACI INPUT BUFFER Determines whether to trace the ACI input buffers at execution time in Trace Browse.	NO	Yes	No
ACITRACEOUT	TRACE ACI OUTPUT BUFFER Determines whether to trace the ACI output buffers at execution time in Trace Browse.	NO	Yes	No
ADABASECHOCLIENT	TRACE ADABAS ECHO CLIENT TRACE REQUESTS Causes the client trace information to be echoed to Trace Browse.	NO	Yes	No
ADABASTRACE	TRACE ADABAS EVENTS Specifies whether to trace ADABAS events.	NO	Yes	No
ADABASTRACEALLCMDS	TRACE ADABAS ALL ADABAS COMMANDS Causes all ADABAS commands to be logged in Trace Browse.	NO	Yes	No
DBTXNTRACEBUFFER	TRACE DB TRANSACTION SQL BUFFERS Controls whether the database transaction program traces SQL buffers.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
DEBUGATMD	DEBUG SERVICE SUBTASK DRIVER ROUTINE If set to 0N, diagnostic trace messages are issued from the product service subtask manager routine OPATMD and various routines which schedule work in service subtasks.	OFF	Yes	No
DEBUGHWUSAGEMON	DEBUG FLAG FOR HARDWARE USAGE MONITOR If set to 0N, detailed debug trace data is written by the check limits hardware usage monitor interval processing routines.	OFF	Yes	No
DEBUGSGMG	DEBUG FLAG FOR SGMG ROUTINE	OFF	Yes	No
DEBUGTRCMTC	DEBUG xDBC TRACE CALLER STACK Causes COTRCMTC to output a stack-trace message before creating new trace messages when this parameter is set to *ON*. The messages traced by COTRCMTC have no free space for a stack trace, so this parameter allows for a caller traceback to be produced.		YES	NO
DECODETRACE	TRACE ASCII-TO-EBCDIC DECODING Indicates whether the ASCII-to-EBCDIC decoding routines should trace input/output processing. This parameter is the default for inbound HTTP request parsing.	NO	Yes	No
DSCLIENTTRACE	TRACE DSCLIENT INTERFACE Includes information about internal state changes of the DS Client server in the trace.		YES	NO
DSCLIENTTRACEAPI	TRACE DSCLIENT API REQUESTS Makes the DS Client API to perform additional tracing.		YES	NO
DSCLIENTTRACEDB	TRACE DSCLIENT DEBUG MESSAGES Includes DS Client processing debugging messages in the trace.		YES	NO
DSCLIENTTRACESQL	TRACE DSCLIENT SQL BLOCKS Formats all the related SQL blocks to server trace after each DS CLIENT SQL request when this parameter is set to *YES*.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
ENCODETRACE	TRACE EBCDIC-to-ASCII ENCODING Indicates whether the EBCDIC-to-ASCII encoding routines should trace input/output processing. This parameter is the default for WWW rule executions and may be overridden using the ENCTRACE keyword for WWW rule definitions.	NO	Yes	No
IDFREPLYMSGTRACE	TRACE IDF REPLY MESSAGE OPERATIONS Traces DRDA DSS packet open and codepoint open calls that are used to reply to a DRDA request.		YES	NO
MAPREDUCETRACE	TRACE MAP REDUCE INTERFACE Includes internal state changes of MAP REDUCE processing in the trace.		YES	NO
MAPREDUCETRACEDB	TRACE MAP REDUCE DEBUG MESSAGES Controls if MAP REDUCE processing traces debugging messages.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
MFLPRIORITYHIGHLEVEL	MICROFLOW HIGH IMPORT TRACE RECORDING LEVEL Controls the granularity and verbosity of Microflow event recording for HIGH importance events. This option can restrict or unfetter MFL trace recording of HIGH importance events. HIGH importance events are normally those that interact with the overall z/OS LPAR; for example, Data Virtualization's End-of-Memory cleanup routines, SSI intercepts, or end-of-task cleanup for external address spaces. The system determines the completion state represented by the event using the return code value being logged. This results in each event having SUCCESS, WARNING, or FAILURE status. The event's importance setting of HIGH then selects this option to control the verbosity of the trace recording. You can select one of the following options for this parameter: • DEBUG: Record ALL completion states; Extended tracing enabled for all events. • VERBOSE: Record ALL completion states; Extended tracing for WARNING and FAILURE completions; SUCCESS completions use non-extended recording. • CHECKOUT: Record only WARNING and FAILURE completions; Omit all SUCCESS completions; WARNING and FAILURE both use extended recording. • NORMAL: Record only WARNING and FAILURE completions; Omit all SUCCESS completions; Only FAILURE completions use extended recording. • TERSE: Trace recording only for FAILING completions; Enable extended tracing for FAILUREs; WARNING and SUCCESS completions are not traced. • RESTRICT: Trace recording only for FAILING completions; All extended tracing is disabled. • PREVENT: No recording is performed for HIGH importance.	VERBOSE	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
MFLPRIORITYLOWLEVEL	MICROFLOW LOW IMPORT TRACE RECORDING LEVEL Controls the granularity and verbosity of Microflow event recording for LOWER importance events. This option can restrict or unfetter MFL trace recording of HIGH importance events. LOW importance events are normally those which relate to the health and execution status of a single Data Virtualization Server transaction of task. Abends in user RPC programs or an authorization failure are examples of low priority events. **MFLPRIORITYLOWLEVEL** accepts the same parameters as the **MFLPRIORITYHIGHLEVEL** start-up parameter. See the discussion there for details on the option settings available and the control each exerts.	NORMAL	Yes	No
MFLPRIORITYMEDLEVEL	MICROFLOW MEDIUM IMPORT TRACE RECORDING LEVEL Controls the granularity and verbosity of Microflow event recording for MEDIUM importance events. This option can restrict or unfetter MFL trace recording of HIGH importance events. MEDIUM importance events are normally those which control the overall operation and health of Data Virtualization Server. This includes initialization and termination events, abnormal service task terminations, storage usage monitoring, and so on. **MFLPRIORITYMEDLEVEL** accepts the same parameters as the **MFLPRIORITYHIGHLEVEL** parameter. See the discussion there for details on the option settings available and the control each exerts.	VERBOSE	Yes	No
PARALLELIOTRACE	TRACE ACI PARTNER STATE CHANGES Controls if internal state changes of Parallel I/O processing will be traced.		YES	NO
PARALLELIOTRACEDB	TRACE ACI PARTNER DEBUG MESSAGES Controls if Parallel I/O processing trace debugging messages.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
RULETRACE	TRACE SEF RULE PROCESSING Causes after-execution tracing to be performed for SEF event/rule processing. If set to NO, only the before-execution trace record is logged. The default value is strongly recommended for Data Virtualization.	YES	Yes	No
SMFFULLSQL	TRACE FULL SQL SOURCE IN SMF Controls how much SQL source is included in SMF records. If set to YES, then the full SQL source is always included in each SMF record. If set to NO, then only the first 256 bytes of the SQL source are included in each SMF record. **Note:** In practice only about 32,000 bytes of SQL source can be included in an SMF record.	NO	Yes	No
SMFGENERICUSERIDS	SMF GENERIC USERIDS Controls whether the generic Userids supplied by any client connection (TLS enabled or not) are accepted and placed in displays and SMF Records. These generic userids are not used for authorization unless the rules concerning TLS userids are met.	NO	Yes	No
SMFNUMBER	SMF RECORD NUMBER	0	Yes	No
SMFTRACEASTEXT	TRACE SMF RECORDS AS TEXT Controls the tracing of SMF records. If set to NO, then SMF records are not copied into Trace Browse as text records. SMF records are only copied into Trace Browse for debugging purposes. If set to YES, then each SMF record is copied into Trace Browse just before it is written out to SMF. Set this parameter to YES only to debug SMF record problems.	NO	Yes	No
SMFTRANSACT	SMF PER-TRANSACTION RECORDING Controls the creation of SMF transaction records. If this parameter is set to YES, then an SMF record is created for each inbound client request. If this parameter is set to NO, then no per-transaction records is created. Each SMF transaction record contains information about all of the work done on behalf of the client. The inbound client request may have caused zero, one, or more SQL operations to be executed.	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
SQLENGDEBUG2A	TRACE SQL DB ACI CONVERSATION Traces DB I/O operations. Data is obtained from Legacy SQL by calling COPRCUBU. This parameter enables tracing of the calls required, and will also dump the rows as they are returned.		YES	NO
SQLENGDEBUG2I	TRACE SQL DB I/O Traces DB I/O operations. Data is obtained from Legacy SQL by calling COPRCUBU. This parameter enables tracing of the calls required, and will also dump the rows as they are returned.		YES	NO
SQLENGDEBUG2IRW	TRACE SQL DB ROW DATA Traces DB I/O operations. Data is obtained from Legacy SQL by calling COPRCUBU. This flag enables tracing of the calls required, and will also dump the rows as they are returned.		YES	NO
SQLENGDEBUGAIO	TRACE SQL ADABAS I/O Includes Adabas I/O information such as address and length of each Adabas I/O operation, Adabas I/O data in the trace.		YES	NO
SQLENGDEBUGCA	TRACE SQL CVCA/CVCE AREA Includes the CVCA/CVCE area used by native VSAM and CICSVSAM access in the trace.		YES	NO
SQLENGDEBUGCIO	TRACE SQL EXCI/CICS I/O Includes EXCI/CICS I/O information such as address and length of each EXCI/CICS I/O operation, and EXCI/CICS I/O data buffers in the trace.		YES	NO
SQLENGDEBUGCM	TRACE SQL DB FULL CMBUS Includes the full CMBUs passed to and received from COPRCUBU for SQL DB access in the trace.		YES	NO
SQLENGDEBUGD2S	TRACE SQL GENERATED STATEMENTS Display the SQL fields generated for DB access when this parameter is set to *YES*.		YES	NO
SQLENGDEBUGDE	TRACE SQL OPDM/OPDE BLOCKS Displays additional information about virtual OPDM and OPDE blocks, that are built to handle OCCURS and OCCURS DEPENDING ON along with a few other cases.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
SQLENGDEBUGIDMSACI	TRACE SQL IDMS ACI SERVER Displays the flow between the SQL Engine and an IDMS ACI server task.		YES	NO
SQLENGDEBUGIMSACI	TRACE SQL IMS ACI SERVER Displays the flow between the SQL Engine and an IMS ACI server task.		YES	NO
SQLENGDEBUGIMSACIS	TRACE SQL IMS ACI PSB Traces start/end conversation and psb schedule/termination.		YES	NO
SQLENGDEBUGIMSIO	TRACE SQL IMS I/O Display additional IMS I/O information. If this option is set, then IMS I/O operations will be traced in greater detail. The address, length, and keys of each IMS I/O operation will be traced. The IMS data buffers will also be traced.		YES	NO
SQLENGDEBUGKY	TRACE SQL KEY RANGE DATA Includes the key range blocks in the trace.		YES	NO
SQLENGDEBUGPL	TRACE SQL SHOW PARAMETER LISTS Includes parameter list information when this parameter is set to *ON*.		YES	NO
SQLENGDEBUGRWDT	TRACE SQL CMBU ROW DATA Enables tracing of row data in a CMBU when this parameter is set to *YES*.		YES	NO
SQLENGDEBUGSEQIO	TRACE SQL SEQUENTIAL I/O Includes information such as address and length of each sequential I/O operation and sequential I/O data buffers in the trace when this parameter is set to *YES*. The will also be traced.		YES	NO
SQLENGDEBUGSQL	TRACE SQL INTERNAL SQL Makes the internal SQL fields passed to Prepare and Execute Immediate will be included in the server trace when this parameter is set to *YES*.		YES	NO
SQLENGDEBUGTC	TRACE SQL COLUMN INFORMATION Includes additional information about the columns that are used to create the data record.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
SQLENGDEBUGTF	TRACE SQL INDEX TREE PROCESSING Includes enhanced filtering in the trace.		YES	NO
SQLENGDEBUGTFDT	TRACE SQL INDEX TREE PROCESSING DETAIL Includes detailed information about enhanced filtering in the trace.		YES	NO
SQLENGDEBUGTI	TRACE SQL ENHANCED INTERNAL PROCESSING Includes SQL enhanced internal processing in the trace.		YES	NO
SQLENGDEBUGTIDT	TRACE SQL ENHANCED INTERNAL PROCESSING DETAIL Includes enhanced internal processing details in the trace.		YES	NO
SQLENGDEBUGTJ	TRACE SQL ENHANCED JOIN PROCESSING Includes enhanced join in the trace.		YES	NO
SQLENGDEBUGTJDT	TRACE SQL ENHANCED JOIN PROCESSING DETAIL Includes detailed information about enhanced indexing in the trace.		YES	NO
SQLENGDEBUGTK	TRACE SQL ENHANCED KEY BUILD PROCESSING Enables tracing for enhanced key processing.		YES	NO
SQLENGDEBUGTKDT	TRACE SQL ENHANCED KEY BUILD PROCESSING DETAIL Includes detailed information about enhanced key trace.		YES	NO
SQLENGDEBUGTO	TRACE SQL ENHANCED OPTIMIZATION Includes enhanced optimization in the trace.		YES	NO
SQLENGDEBUGTODT	TRACE SQL ENHANCED OPTIMIZATION DETAIL Includes detailed information about enhanced optimization in the trace.		YES	NO
SQLENGDEBUGTW	TRACE SQL ENHANCED WHERE PROCESSING Includes SQL enhanced where in the trace.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
SQLENGDEBUGTWDT	TRACE SQL ENHANCED WHERE PROCESSING DETAIL Includes detailed information about SQL enhanced where in the trace.		YES	NO
SQLENGDEBUGTX	TRACE SQL ENHANCED INDEXING Includes enhanced indexing in the trace.		YES	NO
SQLENGDEBUGTXDT	TRACE SQL ENHANCED INDEXING DETAIL Includes detailed information about enhanced indexing in the trace.		YES	NO
SQLENGDEBUGVIO	TRACE SQL VSAM I/O Includes additional VSAM I/O information such as address, VSAM data buffers, length, and keys of each VSAM I/O operation in the server trace when this parameter is set to *YES*.		YES	NO
SQLENGTRACEAI	Lists the aliases returned from the SQL Engine GETALIASES VTB event when this parameter is set to *YES*.		YES	NO
SQLENGTRACECI	TRACE SQL ENGINE CICS OPERATIONS Enables CICS tracing. CICS operations done on behalf of the ANSI SQL 92 Engine is traced in Trace Browse.	NO	Yes	No
SQLENGTRACECO	TRACE SQL ENGINE COLUMN OPERATIONS Enables Virtual Table column tracing.	NO	Yes	No
SQLENGTRACECS	TRACE SQL CCSID CONVERSIONS Enables tracing of SQL CCSID conversions.		YES	NO
SQLENGTRACECT	TRACE ANSI SQL 92 CATALOG OPERATIONS Enables catalog tracing.	NO	Yes	No
SQLENGTRACECV	TRACE SQL DATA CONVERSIONS Enables tracing of SQL data conversions.		YES	NO
SQLENGTRACEIO	TRACE SQL ENGINE I/O OPERATIONS Enables I/O tracing.	NO	Yes	No
SQLENGTRACEKY	TRACE SQL ENGINE KEY OPERATIONS Enables key tracing.	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
SQLENGTRACELVL	TRACE ANSI SQL 92 TRACE LEVEL Sets the trace level.Available options are: • DETAIL • INFORMATION • WARNING • ERROR • SEVERE • FATAL • NONE	NONE	Yes	No
SQLENGTRACEME	TRACE SQL ENGINE MEMORY OPERATIONS Enables memory (get / free) tracing.	NO	Yes	No
SQLENGTRACEMR	TRACE SQL MAP REDUCE PROCESSING Enables map reduce tracing when this parameter is set to *YES*.		YES	NO
SQLENGTRACEPS	TRACE ANSI SQL 92 PSB/PCB SELECTION Enables IMS PSB/PCB selection tracing.	NO	Yes	No
SQLENGTRACEPT	TRACE SQL SQL PARSE TREE Set the SQLENGTRACETR option to display the SQL statement parse tree. The trace displays how the SQL Engine interpreted the SQL statement.		YES	NO
SQLENGTRACERG	TRACE SQL RANGE OPERATIONS Enables tracing of SQL map reduce DRDA range processing when this parameter is set to *YES*.		YES	NO
SQLENGTRACERS	TRACE SQL RUNSTATS PROCESSING Enables tracing of SQL engine runstats processing.		YES	NO
SQLENGTRACESQ	USE THE SQL ENGINE SQL TRACING Enables the SQL tracing provided by the ANSI SQL 92 Engine using a callback.	NO	Yes	No
SQLENGTRACESS	TRACE SQL IMS SSA STRINGS Enables IMS Segment Search Argument tracing when this parameter is set to *ON*.		YES	NO
SQLENGTRACETKEX	TRACE SQL TOKEN ENTRY/EXIT VALUES Traces token entry/exit values when this parameter is set to *YES*.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
SQLENGTRACETR	TRACE SQL ENGINE TRANSLATE OPERATIONS Enables translate tracing.	NO	Yes	No
SQLENGTRACEVR	TRACE SQL ENGINE VIRTUAL OPERATIONS Enables Virtual Table tracing.	NO	Yes	No
SQLENGTRACEVS	TRACE SQL VSAM AND SEQ I/O STATISTICS Displays native VSAM and sequential I/O operation statistics. The trace message displays the number of read operations and the number of records rejected by the post-read exit program, if present.		YES	NO
SQLENGTRACEYX	TRACE SQL ENGINE MODULE ENTRY/EXIT Enables function entry and exit tracing. This option only works if a special version of the ANSI SQL 92 Engine has been built with tracing calls built-in.	NO	Yes	No
THREADLEVELTRACE	ISOLATE MODULE TRACE TO THREAD LEVEL If set to YES, TRACEENTRY, TRACEEXIT and TRACEDATA isolate tracing to one or more enabled subtask threads. If set to N0, these routines generate tracing for all exits in the entire product.	NO	Yes	No
THREADLEVELTRACETCB	THREAD LEVEL TRACE TCB ADDRESS	X'00000000'	Yes	No
TRACE	PRODUCT TRACE OPTION Sets the overall level of communication (LU 6.2 and/or TCP/IP) tracing for the product. Trace messages generated using this parameter are sent to the MVS log, not to Trace Browse. Use of this parameter is not recommended. Set this parameter only under the specific guidance of Customer Support.	BOTH	Yes	No
TRACE24GETS	ONLY TRACE 24-BIT GETMAIN STR EVENTS Controls whether only 24-bit GETMAIN STR events are traced. If set to YES, only 24-bit GETMAIN STR events are traced using Trace Browse. Note, that the event type is STR. If set to N0, then all STR events from the system trace are traced including 24-bit GETMAINs.	YES	Yes	No
TRACEABENDEVENTS	TRACE ABEND EVENTS	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACEABENDRETRYINFO	TRACE ABEND RETRY INFORMATION Controls whether the retry registers and other information is traced when an enabled retry stack frame can be located during ESTAE recovery processing. The retry information, if any, is traced along with the original ABEND SDWA image, when possible, even if retry is not possible and the ABEND is percolated. This parameter is ignored when **TRACEABENDTIME** is set to LATE, because the retry information is already included in traces made late during recovery processing.	YES	Yes	No
TRACEABENDSDWARC1	TRACE ABEND SDWARC1 IMAGE Controls whether the SDWARC1 control block image is traced for ABEND events. **TRACEABENDEVENTS** must also be on. The SDWARC1 control block contains access and control register values at the point of an abnormal termination. It is strongly recommended that this option remain set to YES.	YES	Yes	No
TRACEABENDSDWARC4	TRACE ABEND SDWARC4 IMAGE Controls whether the SDWARC4 control block image is traced for ABEND events. **TRACEABENDEVENTS** must also be on. The SDWARC4 control block contains 64-bit register values at the point of an abnormal termination, and/or retry registers if a retry is attempted following the abnormal termination. It is strongly recommended that this option remain set to YES.	YES	Yes	No
TRACEABENDTIME	TRACE ABEND EVENT TIMING Controls whether tracing for ABEND events is performed early or late in the product's ABEND recovery routines. If set to LATE, the ABEND event tracing of SDWA, SDWARC1, and SDWARC4 blocks occur after it is definitively determined whether a retry or percolation occurs. If set to EARLY, the ABEND event tracing occurs once the outcome can be anticipated, but prior to a final decision. Use the EARLY setting to get diagnostics if you experience ABENDs in the recovery routine.	LATE	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACEABOVETHEBAR	TRACE ABOVE THE BAR STORAGE REQUESTS When set to YES, traces ARV64 macro calls for storage requests for above the bar storage.	NO	Yes	No
TRACEACEECHANGES	TRACE TASK-LEVEL ACEE CHANGES Turns on an internal trace of ACEE pointer alterations. ACEE pointer alterations are used by the server to reset the effective Userid under which transactions are run. Set this parameter only under the specific guidance of Customer Support.	NO	Yes	No
TRACEADABASFULLDATA	Set the TRACEADABASFULLDATA parameter to trace full SQL ADABAS data into Server Trace.		YES	NO
TRACEALLOCABOVEBAR	TRACE ABOVE THE BAR STORAGE SUBALLOCATION Traces storage suballocation calls for above the bar storage. Valid values are YES and NO.	NO	Yes	No
TRACEAPPCDATA	TRACE FULL APPC/MVS DATA Controls whether the full APPC/MVS data for APPC/MVS events is traced or not. If this set to YES, then the complete APPC/MVS data for APPC/MVS events are traced using Trace Browse. If set to NO, then the full APPC/MVS data is not traced.	NO	Yes	No
TRACEAPPCMVSEVENTS	TRACE APPC/MVS EVENTS	YES	Yes	No
TRACEAPPCMVSMN	TRACE APPC/MVS MONITOR Controls whether the APPC/MVS Monitor data collection APIs are to be traced. This parameter should only be turned on if the monitor is not functioning correctly.	NO	Yes	No
TRACEAPPCMVSSR	TRACE APPC/MVS SEND/RECV	NO	Yes	No
TRACEASMFREQUESTS	TRACE ASMF REQUEST PROCESSING Controls tracing of in-bound request processing by the (ASMF) Automated State Management Facility. Restoration operations are traced when this parameter is set. Only unnecessarily in-bound processing generates a trace message if this parameter is off.	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACEASMFRESPONSE	TRACE ASMF RESPONSE/EOT PROCESSING Controls tracing of out-bound Automated State Management Facility (ASMF) operations. If set to NO, these operations are not traced unless unsuccessful. If set to YES, all response-time and end-of-transaction-time processing by the ASMF facility is traced.	NO	Yes	No
TRACEAUTHEVENTS	TRACE AUTHORIZATION EVENTS	NO	Yes	No
TRACEBLISQL	TRACE Z/SERVICE BLI SQL If set to YES, formats all the related SQL blocks to Trace Browse after each BLI SQL request.	NO	Yes	No
TRACEBROWSEAUTHSKIP	SKIP OUTPUT OF SUCCESSFUL TRACEBROWSE CHECKS If set to YES, authorization events which check access to the xxx.TRACEBROWSE and xxx.TRACEDATA resources are not recorded and skipped if they complete successfully (that is, if access is not completely denied). These resources are used to check a user's authorization to access Trace Browse. In cases where trace users may be searching through many panels of information, tracing of the associated resources tends to clutter the trace with unrelated records. Setting this option eliminates one of the chief sources of Trace Browse "noise" that may obscure the user's research.	NO	Yes	No
TRACEBROWSEGROUP1	TRACE BROWSE FLAG GROUP 1	X'226EB07E	Yes	No
TRACEBROWSEGROUP2	TRACE BROWSE FLAG GROUP 2	X'580FB332	Yes	No
TRACEBROWSEGROUP3	TRACE BROWSE FLAG GROUP 3	X'E8004F00	Yes	No
TRACEBROWSEGROUP4	TRACE BROWSE FLAG GROUP 4	X'00000000'	Yes	No
TRACEBROWSEGROUP5	TRACE BROWSE FLAG GROUP 5	X'00000000'	Yes	No
TRACEBROWSEGROUP6	TRACE BROWSE FLAG GROUP 6	X'00000000'	Yes	No
TRACEBROWSEGROUP7	TRACE BROWSE FLAG GROUP 7	X'00000000'	Yes	No
TRACEBROWSEGROUP8	TRACE BROWSE FLAG GROUP 8	X'00000000'	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACECABEXTRACT	TRACE DB2 CONNECTION STATUS EXTRACT Traces CAB and simulated CAB flags. If set to YES, each call to extract DB2 connection status flags is traced.	NO	Yes	No
TRACECEEPIPI	TRACE CEEPIPI CALLS If set to YES, traces calls and enclave status for calls to OPLERU, the interface to the CEEPIPI routine. CEEPIPI is the interface LE/370 enabled code, such as C and COBOL.	NO	Yes	No
TRACECEVENTS	TRACE CLIENT PROGRAM EVENTS	YES	Yes	No
TRACECICSEVENTS	TRACE CICS EVENTS	YES	Yes	No
TRACECLIENTHTTPAPI	TRACE CLIENT HTTP API EVENTS Specifies tracing of HTTP client API calls made when sending a client HTTP request. Note that tracing client API calls also traces some of the headers and data sent for the request, so separately tracing HTTP client headers and HTTP client data may be redundant. There are more API calls, so tracing may be needed to diagnose some problems. Tracing Headers and Data, below, traces ALL the Headers and Data, while the API trace traces only the Headers or Data sent or retrieved by the application.	NO	Yes	No
TRACECLIENTHTTPSTATS	TRACE CLIENT HTTP STATISTICS Specifies tracing of HTTP client statistics after processing a client HTTP request.	NO	Yes	No
TRACECLIENTRECVDATA	TRACE CLIENT HTTP DATA RECEIVED Specifies tracing of HTTP client data received after sending a client HTTP request.	NO	Yes	No
TRACECLIENTRECVHDR	TRACE CLIENT HTTP HEADERS RECEIVED Specifies tracing of HTTP client headers received after sending a client HTTP request.	NO	Yes	No
TRACECLIENTSENDDATA	TRACE CLIENT HTTP DATA SENT Specifies tracing of HTTP client data sent when sending a client HTTP request.	NO	Yes	No
TRACECLIENTSENDHDR	TRACE CLIENT HTTP HEADERS SENT Specifies tracing of HTTP client headers sent when sending a client HTTP request.	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACECPOBJECTS	TRACE DRDA CODEPOINT OBJECTS Traces the cause codepoint related objects following trace of a codepoint read, write, or navigation flow report.		YES	NO
TRACECPREADBUFFER	TRACE DRDA CODEPOINT READ BUFFER Includes the receive buffer after the codepoint read trace.		YES	NO
TRACECPWRITEBUFFER	TRACE DRDA CODEPOINT WRITE BUFFER Includes the send buffer after the codepoint write trace.		YES	NO
TRACECURSOR	TRACE CURSOR STATUS	NO	Yes	No
TRACECURSORADDRESS	TRACE CURSOR ADDRESS	NO	Yes	No
TRACECURSORNUMBER	TRACE SQL EVENTS WITH CURSOR NUMBER Places the cursor number in the SQL event trace text message when this parameter is set to *YES*.		YES	NO
TRACEDASPOPS	TRACE DATASPACE OPERATION Causes dataspace management operations to be traced.	NO	Yes	No
TRACEDATA	TRACE MODULE DATA Controls whether module data trace is on.	X‘07FE’	Yes	No
TRACEDB2DIRDATAP	TRACE DB2-DIRECT DATA PAGES Traces DB2 linear dataset row data pages DB2 direct query processing.		YES	NO
TRACEDB2DIRDICTP	TRACE DB2-DIRECT DICTIONARY PAGES Traces DB2 linear dataset compression dictionary pages during DB2 direct open processing.		YES	NO
TRACEDB2DIROPEN	TRACE DB2-DIRECT OPEN CONTROL BLOCKS Traces DB2 linear dataset header page and control blocks used to process DB2 linear datasets during file open processing.		YES	NO
TRACEDB2DIRSEGP	TRACE DB2-DIRECT SEGMENT PAGES Traces DB2 linear dataset segmented space map pages during DB2 direct open processing.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
TRACEDB2DIRSTATS	TRACE DB2-DIRECT STATISTICS Traces DB2-DIRECT statistics at the end of each DB2-DIRECT SQL query.		YES	NO
TRACEDETACHEVENTS	TRACE DETACH EVENTS	YES	Yes	No
TRACEDISABLEEVENTS	TRACE DISABLE EVENTS	YES	Yes	No
TRACEDIVEVENTS	TRACE DIV MAP AND UNMAP EVENTS Controls tracing of the MAP and UNMAP functions of the DIV macro for Trace Browse archiving.	NO	Yes	No
TRACEDRDACODEPOINT	TRACE DRDA CODEPOINT READ/WRITE If set to YES, then DRDA codepoint read/write operations are traced.	NO	Yes	No
TRACEDRDACONVERT	TRACE DRDA UNICODE CONVERSION SVC REQUEST Includes information about each Unicode Conversion Service codepage conversion operation in the trace.		YES	NO
TRACEDRDADDESBLOK	TRACE DRDA DESCRIPTORS If set to YES, the descriptors for result set columns and bound parameters are traced at various locations in the DRDA interface code. If set to NO, tracing is suppressed.		Yes	No
TRACEDRDARSETBLOK	TRACE DRDA RESULT SET OBJECTS Includes the result set objects for DRDA processing at various points in the DRDA interface when this parameter is set to *YES*.		YES	NO
TRACEDRDASTMTS	TRACE DRDA STMT OBJS IN HLI INTERFACE If set to YES, statement objects used in processing simulated DSNHLI requests through the DRDA interface are traced at entry and exit.		Yes	No
TRACEDSNHLICALLS	TRACE DSNHLI CALLS If set to YES, each call to the DSNHLI is traced. This includes simulated calls made for DRDA process. If set to NO, calls are not traced.	NO	Yes	No
TRACEDSSPACKETRECV	TRACE DRDA DSS DEPACKETIZING Includes DRDA receive DSS depacketizing operations in the trace.		YES	NO
TRACEENABLEEVENTS	TRACE ENABLE EVENTS	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACEENFEVENTS	TRACE ENF EVENTS Controls whether events presented to the ENF listener exit will be traced.		YES	NO
TRACEEXCEPTIONEVENTS	TRACE EXCEPTION EVENTS	YES	Yes	No
TRACEEXCIDPLEVENTS	TRACE EXCI DPL EVENTS	NO	Yes	No
TRACEEXCIEVENTS	TRACE EXCI EVENTS	YES	Yes	No
TRACEEXPECTED47B	TRACE SRB EXPECTED S47B ABENDS When set to YES, Data Virtualization Server traces all S47B ABENDs encountered during operation. When set to NO, expected S47B ABENDs (those that result from SERVER-ISSUED PURGEDQ of an SRB) are not traced.	NO	Yes	No
TRACEEXTERNTRACEDATA	TRACE EXTERNAL TRACE DATA Includes the trace data from the driver sent on the client connection or the trace data sent from an ACI JVM to the server in the server trace when this parameter is set to *Yes*.		YES	NO
TRACEFILEEVENTS	TRACE FILE EVENTS Controls whether file-related processing events are logged to the wrap-around trace.	YES	Yes	No
TRACEFILEINTERNALS	TRACE FILE INTERNAL EVENTS When set to YES, file-related processing generates detailed tracing for internal requests, responses, and internal request re-routing.	NO	Yes	No
TRACEFULLDPLDATA	TRACE FULL DPL DATA Controls whether the entire COMMAREA for DPL events is traced. If this parameter is set to YES, then the complete COMMAREA for DPL events are traced using Trace Browse. If this parameter is set to NO, then the full COMMAREA are not traced.	NO	Yes	No
TRACEFULLLOGONDATA	TRACE FULL LOGON AUTHORIZATION EVENT DATA Causes the complete authorization data for logon events to be traced. If set to NO, some of the logon authorization data is truncated because it cannot fit in a single trace record.	NO	Yes	No
TRACEFULLOPFB	TRACE FULL OPFB FILE OPERATIONS Specifies that OPFB operations trace full data and file block contents.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
TRACEFULLREADDATA	TRACE ALL SEGMENTS OF READ Controls whether all segments of an OE Sockets read are traced. As each segment of an OE Socket is read, the information regarding that segment and the first *xxx* bytes of data is optionally traced. Normally, this does not present a problem. But if large LOBs are being transmitted to Data Virtualization, a large number of secondary READ EXECUTED trace records are generated which can clutter up the Trace Browse. If set to NO, only the first segment is traced.	NO	Yes	No
TRACEFULLRRSDATA	TRACE FULL RRS DATA Controls whether the entire RRSAREA for RRS events is traced. If this parameter is set to YES, then the complete RRSAREA for RRS events are traced using Trace Browse. If this parameter is set to NO, then the full RRSAREA are not traced.	NO	Yes	No
TRACEFULLXCFDATA	TRACE FULL XCF DATA Controls whether the entire XCCAAREA for XCF events is traced. If this parameter is set to YES, then the complete XCCAAREA for XCF events are traced using Trace Browse. If this parameter is set to NO, then the full XCCAAREA is not traced.	NO	Yes	No
TRACEFULLZEDC	TRACE FULL ZEDC COMPRESSION Specifies that ZEDC compression trace arguments and return codes and all data.		YES	NO
TRACEGLVEVENTS	TRACE GLOBAL VARIABLE EVENTS	YES	Yes	No
TRACEHLLENQDEQ	TRACE PRODUCT HLL ENQ/DEQ ACTIVITY If set to YES, any ENQ or DEQ operations generated by HLL PRODUCT components via the internal-use-only API module are traced.	NO	Yes	No
TRACEHSMEVENTS	TRACE DFHSM EVENTS AS FILE EVENTS Controls whether DFHSM request processing operations are traced as FILE events. The **TRACEFILEEVENT** parameter must also be set to YES for this parameter to have any effect.	NO	Yes	No
TRACEIBMMQEVENTS	TRACE IBM/MQ EVENTS	YES	Yes	No
TRACEIBMMQGP	TRACE IBM/MQ MGET/MPUT EVENTS	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACEIDFCCSIDINFO	TRACE IDF CCSID INFO CALLS Causes IDF to trace reply data during CCSID information calls.		YES	NO
TRACEIDFCODEPOINTNAV	TRACE IDF CODEPOINT NAVIGATION Causes IDF to trace IDF input processing codepoint processing navigation.		YES	NO
TRACEIDFCOLUMNSQLDA	TRACE IDF COLUMN SQLDA INFORMATION Traces SELECT and stored procedure result set column SQLDA entries and newly prepared cursor blocks.		YES	NO
TRACEIDFCPPAEMIT	TRACE IDF CPPA PARSE ELEMENTS Includes DRDA code points in the trace when the code points are parsed out of consolidated DSS packets.		YES	NO
TRACEIDFCPPAEMITDATA	TRACE IDF CPPA PARSE DATA Includes the data associated with each parsed CPPA in the trace. This parameter requires the TRACEIDFCPPAEMIT parameter to be set to *YES*.		YES	NO
TRACEIDFDSSPARSE	TRACE IDF DSS POST-RECEIVE PARSE ELEMENTS Generates diagnostic traces showing parsed and re-mapped DSS packets		YES	NO
TRACEIDFDSSPARSEDATA	TRACE IDF DSS POST-RECEIVE PARSE DATA Includes the DSS packet data in the trace. This parameter requires the TRACEIDFDSSPARSE to be set to *NO*.		YES	NO
TRACEIDFDSSRECV	TRACE IDF DSS RECEIVE-TIME DEPACKETIZATION Generates diagnostic traces when DRDA DSS packets are received.		YES	NO
TRACEIDFEVENTS	TRACE IDF APPLICATION SERVER EVENTS Includes Integrated DRDA Facility (IDF) DRDA Application Server messages when this parameter is set to *YES*.		YES	NO
TRACEIDFFETCHBLOCKS	TRACE IDF FETCH BLOCKS Causes IDF to trace internal buffers containing result set rows during fetch processing.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
TRACEIDFPACKSTMT	TRACE IDF BOUND PACKAGES/ STATEMENTS Causes IDF to trace package and package statement control blocks during execution.		YES	NO
TRACEIDFSQLCALLS	TRACE IDF SQL CALLS Causes IDF to trace internal request processing areas used to invoke SQL Engine interfaces.		YES	NO
TRACEIDFSQTABLOCKS	TRACE IDF SQTA BLOCKS Includes SQTA blocks in the trace whenever it is created.		YES	NO
TRACEIDFTHREADBLOCK	TRACE IDF THREAD BLOCKS Causes the main IDF processing block to be included in the trace whenever a command request is completed.		YES	NO
TRACEIDFTHREADSETUP	TRACE IDF THREAD SETUP Causes IDF and Metal-C runtime setup for each thread.		YES	NO
TRACEIMSDBBLOCKS	TRACE IMS-DIRECT CONTROL BLOCKS Generates trace/dump messages of used IMS-Direct map reduce discovery blocks when accessed.		YES	NO
TRACEIMSDBREFRESH	TRACE IMS-DIRECT DISCOVERY REFRESH Generates a trace message when IMS-Direct map reduce discovery processing is performed.		YES	NO
TRACEIMSDIRCHASE	TRACE IMS-DIRECT ACI CHASE Traces the next segment to be processed by IMS-Direct.		YES	NO
TRACEIMSDIRCIBUF	TRACE IMS-DIRECT ACI CI BUFFERS Traces VSAM CI buffers when they are read by the IMS-Direct task.		YES	NO
TRACEIMSDIRFETCHRBA	TRACE IMS-DIRECT ACI FETCHRBA Traces the next Relative Byte Address to be processed by IMS-Direct.		YES	NO
TRACEIMSDIRFILEBLKS	IMS-DIRECT CONTROL BLOCKS Traces IMS Direct file blocks		YES	NO
TRACEIMSDIRFILEOPS	TRACE IMS-DIRECT ACI FILE OPERATIONS Traces file operations in IMS-Direct.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
TRACEIMSDIRFLOW	TRACE IMS-DIRECT ACI FLOW CONTROL Traces the ACI task side of IMS-Direct flow control.		YES	NO
TRACEIMSDIRIMBF	TRACE IMS-DIRECT ACI SEND-TIME IMBF Traces IMBF data segments produced by the IMS-Direct task.		YES	NO
TRACEIMSDIRMRBU	TRACE IMS-DIRECT ACI SEND-TIME MRBU Traces MRBU at SEND of buffer from IMS-Direct task.		YES	NO
TRACEIMSDIRNAV	TRACE IMS-DIRECT ACI NAVIGATION Traces navigation of segments in IMS-Direct.		YES	NO
TRACEIMSDIRNEXTRAP	TRACE IMS-DIRECT ACI NEXTRAP Traces the next Root Anchor Point to be processed by IMS-Direct.		YES	NO
TRACEIMSDIRSETUPBLKS	TRACE IMS-DIRECT MAP REDUCE SETUP DATA AREAS Includes IMS Map Reduce run time control blocks in the trace.		YES	NO
TRACEIMSDIRSQLFLOW	TRACE IMS-DIRECT SQL ENGINE FLOW CONTROL Traces the SQLEngine task side of IMS-Direct flow control.		YES	NO
TRACEIMSDIRSTATS	TRACE IMS-DIRECT ACI RUNTIME STATISTICS Produces runtime statistics at the end of IMS-Direct processing of a dataset.		YES	NO
TRACEIMSDIRTASKSETUP	TRACE IMS-DIRECT MAP REDUCE TASK SETUP Includes IMS Map Reduce task assignments in the trace.		YES	NO
TRACEIMSDLIEVENTS	TRACE IMS DLI EVENTS	NO	Yes	No
TRACEIMSEVENTS	TRACE IMS EVENTS	YES	Yes	No
TRACEIMSWEBSERVICES	Enables tracing of IMS SLI or IMS BLI module processing at various points, for diagnostic purposes.		Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACEINTERVAL	TRACE INTERVAL PROCESSING Controls the tracing of interval processing. If set to YES, then a text message is written into Trace Browse just before each type of interval processing is performed. If set to NO, then a text message is not added to Trace Browse as part of interval processing. **Note:** Interval processing is performed in either case. This flag should be set to YES only to debug problems with interval processing.	NO	Yes	No
TRACEJAVAEVENTS	TRACE JAVA EVENTS Controls the tracing of Java events, excluding redirected streams.	YES	Yes	No
TRACEJAVASTREAMS	TRACE JAVA STREAMS Controls the tracing of Java streams.	YES	Yes	No
TRACELDUEVENTS	TRACE LDU EVENTS If set to YES, Data Virtualization Server traces Logical Dispatchable Unit (LDU) events. These traces are written as STR-LDU events and include LDU construction, termination, and TCB/SRB mode switches. If set to NO, these events are traced only when results of the operation are unexpected or in error.	NO	Yes	No
TRACELDUMODESWT	TRACE LDU MODE SWTCH When set to YES, Data Virtualization Server traces Logical Dispatchable Unit (LDU) execution dispatchable unit mode switches, written as STR events. If set to NO, these events are not traced.	NO	Yes	No
TRACELDUSIGNALS	TRACE LDU SIGNALS When set to YES, Data Virtualization Server traces Logical Dispatchable Unit (LDU) signal events. These traces are written as STR events. If set to NO, these events are traced only when results of the operation are unexpected or in error.	NO	Yes	No
TRACELOGSTREAM	TRACE LOGSTREAM CALLS When set to YES, Data Virtualization Server traces the results of IXGxxxxx macro calls to the MVS logger. These traces contain the results of the calls.	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACELOGSTREAMB	TRACE LOGSTREAM BEFORE When set to YES, Data Virtualization Server traces IXGxxxx macro calls before they are issued. This may not be as useful as the **TRACELOGSTREAM** tracing.	NO	Yes	No
TRACELOGSTREAMFULL	TRACE FULL LOGSTREAM DATA When set to YES, Data Virtualization Server traces all the data associated with a logstream request.	NO	Yes	No
TRACELU62DATA	TRACE FULL LU 6.2 DATA Controls whether the full LU 6.2 data for LU 6.2 read/write events is traced or not. If set to YES, then the complete LU 6.2 data for LU 6.2 read/write events are traced using Trace Browse. If set to NO, then the full LU 6.2 data is not traced.	NO	Yes	No
TRACELU62DETAIL	TRACE DETAILED LU 6.2 EVENTS	NO	Yes	No
TRACELU62EVENTS	TRACE LU 6.2 EVENTS	NO	Yes	No
TRACELU62RDWR	TRACE LU 6.2 READ/WRITE EVENTS	NO	Yes	No
TRACEMERGE	MERGE SUCCESSFUL FETCH EVENTS	YES	Yes	No
TRACEMERGETHROW	MERGE SUCCESSFUL THROW EVENTS	YES	Yes	No
TRACEMFLEVENTS	TRACE MICROFLOW EVENTS Controls the tracing of MicroFlow (MFL) vents.	NO	Yes	No
TRACEMONGOEVENTS	TRACE MONGODB EVENTS Includes MONGO DB events in the trace when this parameter is set to *YES*.		YES	NO
TRACEMONGOXQ	TRACE MONGODB XQ EVENTS Includes the XQ operations in the Mongo outer XQ interface layer in the trace.		YES	NO
TRACEMONGOXQDETAIL	TRACE MONGODB XQ EVENT DETAIL Includes detailed information about XQ Fetch operations in the trace when this parameter is set to *YES*. When this parameter is set to *NO*, only the end-of-data Fetch request is traced unless an error occurs.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
TRACEMQDATA	TRACE FULL MQ SERIES DATA Controls whether the full MQ Series data for MQGET/MQPUT events is traced. If set to YES, then the complete MQ data for MQ Series MQGET/MQPUT events will be traced using Trace Browse. If set to NO, then the full MQ Series data is not traced.	NO	Yes	No
TRACENOEVENTS	TRACE NO EVENT TYPE EVENTS	NO	Yes	No
TRACENTRY	TRACE MODULE ENTRY Controls whether module entry trace is on.	X‘07FE’	Yes	No
TRACEOEDATA	TRACE FULL OE SOCKETS DATA Controls whether the full OE Sockets data for OE Sockets read/write events is traced. If set to YES, then the complete OE Sockets data for OE Sockets read/write events is traced using Trace Browse. If set to NO, then the full OE Sockets data is not traced.	YES	Yes	No
TRACEOEDRDARW	TRACE OE SOCKETS DRDA READ/WRITE EVENTS If set to YES (strongly recommended), TCP/IP communications via DRDA are traced. If set to NO, DRDA receive and send operations are not traced.	NO Setting to YES is strongly recommended.	Yes	No
TRACEOEEVENTS	TRACE IBM OE SOCKETS EVENTS Controls whether IBM OE Sockets TCP/IP events should be traced. If set to YES, IBM OE Sockets TCP/IP events are traced. If set to NO, then IBM OE Sockets TCP/IP events are not traced.	YES	Yes	No
TRACEOERW	TRACE OE SOCKETS READ/WRITE EVENTS Controls whether IBM OE Sockets TCP/IP Read/Write events should be traced. If set to YES, IBM OE Sockets TCP/IP Read/Write events are traced. If set to NO, then IBM OE Sockets TCP/IP Read/Write events are not traced.	YES	Yes	No
TRACEOERWSTART	TRACE OE SOCKETS R/W EVENT START Controls whether the start of IBM OE Sockets TCP/IP Read/Write events should be traced. If set to YES, then the initiation of IBM OE TCP/IP Read/Write events is traced. If set to NO, then the initiation of IBM OE TCP/IP Read/Write events is not traced.	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACEOPENCLOSE	TRACE OPEN AND CLOSE Controls if file open and close events are logged in the wrap-around trace.		YES	NO
TRACEOPFBCIACCESS	TRACE OPFB CI ACCESS Specifies that VSAM control intervals from CI read and write access will be traced.		YES	NO
TRACEOPFBONENTRY	TRACE OPFB ON ENTRY Specifies that OPFB file operations trace on entry and after the request is performed.		YES	NO
TRACEOPFBOPERATIONS	TRACE OPFB FILE OPERATIONS Specifies that OPFB file operations will be traced.		YES	NO
TRACEOPFBPREEXIT	TRACE OPFB FILE BEFORE EXIT Specifies that OPFB file operations will be traced before calling a user exit.		YES	NO
TRACEOPFBSTARTUPOPS	TRACE OPFB FILE STARTUP OPERATIONS Specifies that OPFB file operations will be traced during startup.		YES	NO
TRACEOTMABUFFERDATA	TRACE OTMA BUFFER CONTENT DATA Controls the tracing of IMS/OTMA buffer contents.	NO	Yes	No
TRACEOTMADETAIL	TRACE OTMA DETAILED EVENTS Controls the tracing of IMS/OTMA detail events.	NO	Yes	No
TRACEOTMAEVENTS	TRACE OTMA EVENTS Controls the tracing of IMS/OTMA events.	NO	Yes	No
TRACEPEALLO	TRACE PAUSE ELEMENT ALLOC/FREE When set to YES, Data Virtualization Server traces allocation and de-allocation of pause elements (PEs) used for TCB and SRB LDU (Logical Dispatchable Unit) control. These traces are written as STR-PEL events. If set to N0, these events are traced only when results of the operation are unexpected or in error.	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACEPEDISPATCH	TRACE PAUSE ELEMENT DISPATCH If set to YES, Data Virtualization Server traces the results of pause element (PE) pause and transfer requests. These traces are written as STR-PEL events. If set to NO, these events are traced only when results of the operation are unexpected or in error.	YES	Yes	No
TRACEPETEST	TRACE PAUSE ELEMENT TEST If set to YES, Data Virtualization Server traces the results of pause element (PE) test requests. These traces are written as STR-PEL events. If set to NO, these events are traced only when results of the operation are unexpected or in error.	NO	Yes	No
TRACEPUBLISH	TRACE Z/EVENTS Controls tracing of Data Virtualization z/Events servers. Specifying YES causes all calls to be traced.	YES	Yes	No
TRACEPUBLISHRULEAPI	TRACE Z/EVENTS RULE API CALLS Controls tracing of the Data Virtualization z/Events rule API calls. If set to YES, z/Events API calls inside PUB rules are traced.	NO	Yes	No
TRACEQSDETAIL	TRACE QS DETAIL EVENTS Specific to the Data Virtualization Query Server. Care should be used when setting this parameter to YES. This parameter causes detail trace records to be written to Trace Browse for every thread connected to a DB2 system that is also connected to the Query Server. At a minimum, one record for each SQL statement is written, whether the statement is of interest to the Query Server. For statements of interest, one record for each GTT, plus two records for each row inserted into the GTT, are written to Trace Browse.	NO	Yes	No
TRACERESPBUFFERS	TRACE HTTP RESP BUFFERING If set to YES, the server generates trace entries for certain HTTP response buffering operations. The trace information is used mostly to diagnose problems when an out-bound HTTP response appears to be incomplete.	NO	Yes	No
TRACEREXXEXEC	TRACE REXX EXECUTION	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACEROWFETCHCOUNT	TRACE DRDA ROW FETCH COUNT Includes the requested row count passed on block fetch requests to DRDA in the trace.		YES	NO
TRACERPCEVENTS	TRACE ODBC CALL RPC EVENTS	YES	Yes	No
TRACERRSAF	TRACE RRSAF REQUESTS If set to YES, an entry is made in Trace Browse for each call to DSNRLI for RRSAF requests.	YES	Yes	No
TRACERRSEVENTS	TRACE RRS EVENTS	YES	Yes	No
TRACESECOPTINT	TRACE SECURITY OPT INTERVAL PROCESSING Controls tracing of SOM intervals.	NO	Yes	No
TRACESECOPTOPS	TRACE SECURITY OPTIMIZER OPERATIONS Controls tracing of SOM operations.	NO	Yes	No
TRACESECOPTSUM	TRACE SECURITY OPT SUMMARY INFORMATION Controls tracing of SOM summary and statistical information.	NO	Yes	No
TRACESECURITYATTRIBS	TRACE WWW SECURITY ATTRIBUTES	YES	Yes	No
TRACESECURITYDATA	TRACE SECURITY DATA Controls tracing of security data. The only current security data is messages from Logon processing. These messages are copied into Trace Browse as text if the flag below is set.	NO	Yes	No
TRACESISBUFFERDATA	TRACE SIS/XCF BUFFER DATA Controls the tracing of SIS/XCF buffer contents.	NO	Yes	No
TRACESISDETAIL	TRACE SIS/XCF DETAIL EVENTS Controls the tracing of SIS/XCF detail events.	NO	Yes	No
TRACESISEVENTS	TRACE SIS/XCF EVENTS Controls the tracing of SIS/XCF events.	NO	Yes	No
TRACESISSTUDIODETAIL	TRACE SIS/STUDIO DETAIL If set to YES, all API routines executed in support of call Data Virtualization_server.	NO	Yes	No
TRACESLISQL	TRACE Z/SERVICE SLI SQL If set to YES, formats all the related SQL blocks to Trace Browse after each SLI SQL request.	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACESQLDIAGDETAIL	TRACE SQL GET DIAGNOSTICS DETAIL Controls whether the detailed information from SQLGetDiagnostics calls are to traced. If set to YES, then the SQL trace record for get diagnostics request contains all information available. If set to NO, the detailed information is not traced.	YES	Yes	No
TRACESQLENGCALLS	TRACE SQLENG CALLS Includes each DSNHLI call to the SQL engine in the trace when this parameter is set to *YES*.		YES	NO
TRACESQLEVENTS	TRACE SQL EVENTS Controls whether SQL events are traced. If this parameter is set to YES, then SQL events are traced using Trace Browse. If set to NO, then SQL events are not traced. **Note:** This parameter does not control the tracing of SQL events from the logging task. SQL events from the logging task are traced as SQM events. SQL events can be filtered using the Trace Browse profile facility.	YES	Yes	No
TRACESQLHIGHLIGHT	TRACE SQL EVENTS WITH HIGHLIGHTING Highlights SQL events in the server trace when this parameter is set to *YES*.		YES	NO
TRACESQLSOURCE	TRACE FULL SQL SOURCE Controls whether the full SQL source for SQL events is traced or not. If set to YES, the complete SQL source for SQL events is traced using Trace Browse. If set to NO, the full SQL source is not traced.	NO	Yes	No
TRACESQMEVENTS	TRACE SQL EVENTS FROM LOGGING Controls whether SQL events from the logging task are traced or not. If set to YES, SQL events from the logging task are traced using Trace Browse. **Note:** The event type is SQM, not SQL. If set to NO, then SQL events from the logging task are not traced. Note that this parameter only controls the tracing of SQL events from the logging task. The tracing of all other SQL events is controlled using the **TRACESQLEVENTS** parameter. SQM events can be filtered using the Trace Browse profile facility.	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACESRBDISPATCH	TRACE SRB DISPATCH If set to YES, Data Virtualization Server traces the SRB schedule requests and SRB terminations. These traces are written as STR-LDU events. If set to NO, these events are traced only when results of the operation are unexpected or in error.	NO	Yes	No
TRACESRPFUNCTION	TRACE SERVICE PROVIDER FUNCTIONS Causes the service requester/provider interface to generate trace messages during internal operations. Set this parameter only under the specific guidance of Customer Support.	NO	Yes	No
TRACESTACK	TRACE STACK USAGE Controls whether stack trace is on.	NO	Yes	No
TRACESTACKONASSERT	TRACE STACK AFTER METAL-C ASSERT Includes the thread stack in the trace after any metal-c assert is traced when this parameter is set to *YES*.		YES	NO
TRACESTATICSQL	TRACE STATIC SQL SOURCE	NO	Yes	No
TRACESTORAGEEVENTS	TRACE STORAGE EVENTS	NO	Yes	No
TRACESTREAMS	TRACE STREAMS Control tracing of streams servers when this parameter is set to *YES*.		YES	NO
TRACESTREAMSARCHIO	TRACE STREAMS ARCHIVE FILE I/O Enables tracing of Streams archive files I/O events.	NO	YES	NO
TRACESTREAMSCAPTURE	TRACE STREAMS CAPTURE Causes detection and recording of events to be traced when this parameter is set to *YES*.	NO	YES	NO
TRACESTREAMSCONVERT	TRACE STREAMS CONVERSION Controls tracing of streams data conversion calls when this parameter is set to *YES*.	NO	YES	NO
TRACESTREAMSDATA	TRACE STREAMS FULL DATA Controls tracing of full publish data for STREAMS events in the server trace when this parameter is set to *YES*.		YES	NO
TRACESTREAMSDEBUG	TRACE STREAMS DEBUG Controls tracing of the Streams module debugging information.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
TRACESTREAMSEVENTIO	TRACE STREAMS EVENT I/O Causes Streams I/O events to be traced when this parameter is set to *YES*.	NO	YES	NO
TRACESTREAMSFLOW	TRACE STREAMS MODULE FLOW Enables tracing of Streams module flow when this parameter is set to *YES*.		YES	NO
TRACESTREAMSWORKIO	TRACE STREAMS WORK FILE I/O Controls tracing of Streams I/O events.	NO	YES	NO

Parameter name	Parameter description	Default value	Update	Output only
TRACESTREVENTS	TRACE STR EVENTS FROM SYSTEM TRACE Controls whether STR traces for system-control events are traced. If set to YES, then STR events related to system control are recorded in Trace Browse. **Note:** The event type is STR. If set to N0, then STR events from the system trace are not traced. For events reflecting a critical failure or error in the overall product architectural controls, this setting is ignored, and the event recorded, regardless the setting. This provides critical debugging information for which a subsequent system, product, or transaction processing failure is presumed likely to follow. This parameter controls many classes of product operational and operating system interface control events. The first is tracing of requests for z/OS LOAD, STORAGE, GETMAIN, FREEMAIN and certain LE requests. The capture of events for this class is controlled by the parameters **PROCESSEP**, **PROCESSPC**, and **PROCESSSVC**. These parameters are only for use under direction of Customer Support. The second is tracing of certain critical RPC program scheduling and control events. and **TRACEPEDISPATCH**. Actual capture of events of this class is controlled by the parameter **RPCMAXTRACE**. The third is tracing of SRB scheduling, dispatch, cleanup, and termination events. Actual capture of events of this class is controlled by the parameter **TRACESRBDISPATCH**. The fourth is tracing of Pause Element Service API requests, which use the IEAVxxx z/OS interfaces. Capture of these events is controlled by the parameters **TRACEPEALLO**, and **TRACEPETESTS**. The fifth is tracing of Logical Dispatchable Unit (LDU) dispatch and control events. Actual capture of these events is controlled by the parameters **TRACELDUEVENTS** and **TRACELDUSIGNALS**.	YES	Yes	No
TRACETEXTEVENTS	TRACE TEXT EVENTS	YES	Yes	No
TRACETODEVENTS	TRACE TOD EVENTS	YES	Yes	No
TRACETSOEVENTS	TRACE TSO EVENTS Controls whether out-board TSO server events are logged to the wrap-around trace.	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
TRACEURL	TRACE INBOUND HTTP REQUESTS If set to YES, each HTTP request message is traced once the message has been received and parsed, and prior to request transaction processing.	YES	Yes	No
TRACEURLBODY	Z/SERVICE URL BODY When set to YES, traces all the body text for a z/Services request. Otherwise, only the HTTP headers are traced.	NO	Yes	No
TRACEURLREAD	TRACE HTTP RECEIVE STATES If set to YES, the server generates trace messages at key landmarks during http request message receive processing. Use of this option may allow you to diagnose problems with in-bound HTTP request messages that the server rejects as malformed. It also traces activity related to persistent session and HTTP pipelined request processing.	NO	Yes	No
TRACEWEBAPIEVENTS	TRACE WEB API EVENTS	YES	Yes	No
TRACEWLMCALLS	TRACE WLM API CALLS Controls tracing of Data Virtualization Server calls to the WLM APIs for transaction management. If set to YES, all calls are traced.	NO	Yes	No
TRACEWSDATASQL	TRACE Z/SERVICE WSDATA SQL If set to YES, formats all the related SQL blocks to Trace Browse after each WSDATA SQL request.	NO	Yes	No
TRACEWTOMODULES	WTO MODULE ENTRY/EXIT MESSAGES	NO	Yes	No
TRACEWWWEVENTS	TRACE WWW EVENTS	YES	Yes	No
TRACEXCFEVENTS	TRACE XCF EVENTS Controls the tracing of coupling facility (XCF) events.	NO	Yes	No
TRACEXIT	TRACE MODULE EXIT Controls whether module exit trace is on.	X‘07FE’	Yes	No
TRACEZEDCCOMPRESSION	Specifies that ZEDC compression traces arguments and return codes.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
TRACEZSREVENTS	TRACE Z/SERVICES (ZSR) EVENTS Can be set to record or suppress recording of ZSR (z/Services) events. Other options can be used to control tracing of individual sub-components or data in the z/Services facility. This global option can be set to N0 to suppress recording of all ZSR events as a group.	YES	Yes	No
TRANSINTTIMINGS	TRACE TIMINGS FOR WWW SERVICES If set to YES, various API routines of Data Virtualization Web Server generate trace records to record entry and exit events Using the **D CPU** command in Trace Browse displays the CPU time column. The CPU timings for these event records are precise, regardless of the setting of the PRECISECPUTIME option. You can use this option to display the amount of CPU time required to process various WWW services, such as buffering a cached file for transmission, or processing HTML extensions. It is recommended that you do not set this option except to periodically collect performance data.	NO	Yes	No
TSOSRVTRACEOPER	TRACE TSOSRV OPERATIONS Indicates whether TSO Server dispatching and control operations should be traced.	NO	Yes	No
VPDTRACEDB	TRACE VPD DEBUG MESSAGES Includes VPD processing in debugging messages.		YES	NO
VPDTRACEREC	TRACE VPD RECORDS Causes VPD to trace at the record level.		YES	NO
VSAMTRACECICS	TRACE VSAM CICS EXECUTION Traces the CICS VSAM program execution in Trace Browse.	NO	Yes	No
WSCICSSLITRACE	TRACE WEB SERVICES SLI DEBUG Can be set to record or suppress recording of the CICS SLI interface module for diagnostic purposes.	NO	Yes	No
WSREXXSLITRACE	TRACE Z/SERVICES SLI REXX Specifies whether to trace or suppress tracing of SLI REXX module processing at various points, for diagnostic purposes.	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
ZCONNECTTRFLG0	Z/OS CONNECT TRACE FLAG 0 Traces information about when z/OS CONNECT related WOLA tasks are processing start and stop activity.		YES	NO
ZCONNECTTRFLG1	Z/OS CONNECT TRACE FLAG 1 Traces information about when z/OS CONNECT related WOLA tasks are processing path activity.		YES	NO
ZCONNECTTRFLG2	Z/OS CONNECT TRACE FLAG 2 Traces information about when z/OS CONNECT related WOLA tasks are processing path messages.		YES	NO
ZCONNECTTRFLG3	Z/OS CONNECT TRACE FLAG 3 Traces information about when z/OS CONNECT related WOLA tasks are processing path start and stop.		YES	NO
ZCONNECTTRFLG4	Z/OS CONNECT TRACE FLAG 4 Traces information about when z/OS CONNECT related WOLA tasks are processing request start and stop.		YES	NO
ZCONNECTTRFLG5	Z/OS CONNECT TRACE FLAG 5 Traces information about when z/OS CONNECT related WOLA tasks are processing request messages.		YES	NO
ZCONNECTTRFLG6	Z/OS CONNECT TRACE FLAG 6 Traces information about the z/OS CONNECT WOLA request and response buffers.		YES	NO
ZCONNECTTRFLG7	Z/OS CONNECT TRACE FLAG 7 Traces the z/OS CONNECT WOLA detailed request processing messages.		YES	NO

Parameter name	Parameter description	Default value	Update	Output only
ZCONNECTTRLEV	Z/OS CONNECT TRACE LEVEL Sets the trace level for the z/OS CONNECT interface facility. The following levels can be set: • 0 - No trace processing will be performed • 1 - Trace request path start and stop processing • 2 - 1 + trace request begin and end processing • 3 - 2 + trace request processing information • 4 - 3 + trace input and output buffer processing		YES	NO
ZSRMBOXEVENTLIMIT	Z/SERVICE PER MAILBOX EVENT RECORDING LIMIT Each z/Services mailbox can optionally impose a limit on the total number of mailbox events written to Trace Browse. Once the limit is reached, no further recording of mailbox request event traces occurs, regardless of the reason or event being logged. This parameter is used to set the initial count limit value for each new mailbox created in the system. When a limit value of ZER0 is set, the count of recorded events is ignored and all eligible events are recorded. Otherwise, a limit value of 1 through 16000000 may be used for this parameter. Generally, you should set a non-zero value for this parameter only when attempting problem diagnosis.	0 EVENTS	Yes	No
ZSRMBOXTRACEABEND	TRACE Z/SERVICE ABENDING MAILBOX REQUESTS Causes failing mailbox requests to be traced, if the failure was a ABEND exception. This option is the system default action for tracing z/Service requests terminating due to an ABEND failure.	YES	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
ZSRMBOXTRACEALLPOST	TRACE Z/SERVICE ALL MAILBOX INTERNAL POSTS If set to YES, causes successful internal mailbox POST requests to be traced to show re-dispatch of waiting receivers. Failing POST requests are always traced unless z/Service event tracing is disabled. This option is the system default for tracing successful z/Service internal POST processing that re-dispatches waiting work units.	NO	Yes	No
ZSRMBOXTRACECMTC	TRACE Z/SERVICE INCLUDE CMTC OPTION If set to YES, causes the related task ‘s CMTC block to be included with certain mailbox event traces. This option is ignored unless full (extended) tracing is enabled (see **ZSRMBOXTRACEFULLDATA**). If set to NO, or when full (extended) tracing is not enabled, CMTC blocks are not included in mailbox traces. This option is the system default for tracing z/Service events.	NO	Yes	No
ZSRMBOXTRACEFAIL	TRACE Z/SERVICE FAILING MAILBOX REQUESTS If set to YES, causes mailbox request exit tracing for failure return codes. This option is the system default for tracing z/Service requests terminated due to a failure.	YES	Yes	No
ZSRMBOXTRACEFULLDATA	TRACE Z/SERVICE MAILBOX EXTENDED DATA If set to YES, causes extended tracing to be performed for z/service trace entries. This causes full data block and buffer content to be traced. If set to NO, z/Service traces are truncated and some diagnostic data may be unrecorded. This option is the system default for tracing z/Service events.	NO	Yes	No
ZSRMBOXTRACESUCCESS	TRACE Z/SERVICE SUCCESSFUL MAILBOX REQUESTS	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
ZSRMBOXTRACEUNDELIVR	TRACE Z/SERVICE UNDELIVERED MESSAGE PURGE If set to YES, causes internal PURGE requests for undelivered messages to be traced. Undelivered messages are purged when the mailbox they reside in is deleted or cleared. Receive PURGE recovery events are always traced unless all z/Service traces are disabled. Receiver PURGE events normally occur due to POST failure, or detection of early task termination when outstanding receive requests remain queued. This option is the system default for tracing undelivered z/Service message PURGE events.	YES	Yes	No
ZSRMBOXTRACEWARN	TRACE Z/SERVICE WARNING MAILBOX REQUESTS If set to YES, causes mailbox request exit tracing for warning return codes. This is the system default for tracing z/Service requests completing with an exception or error.	NO	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
ZSRPRIORITYHIGHLEVEL	TRACE Z/SERVICE HIGH IMPORT TRACE REC. LEVEL Controls the granularity and verbosity of z/Services event recording for HIGH importance events. This option can restrict or unfetter ZSR trace recording of high importance events other than z/Service Mailbox/PC-call traces. HIGH importance events are normally those that interact with the overall z/OS LPAR; for example, Data Virtualization's End-of-Memory cleanup routines, SSI intercepts, or end-of-task cleanup for external address spaces. The system determines the completion state of the event using the return code value. Each event is logged as having SUCCESS, WARNING, or FAILURE status. The event's importance setting of HIGH selects this option to control the verbosity of the trace recording. Select one of the following options: • DEBUG: Record ALL completion states; Extended tracing enabled for all events. • VERBOSE: Record ALL completion states; Extended tracing for WARNING and FAILURE completions. SUCCESS completions use non-extended recording. • CHECKOUT: Record only WARNING and FAILURE completions, which both use extended recording. Omit all SUCCESS completions. • NORMAL: Record only WARNING and FAILURE completions; only FAILURE completions use extended recording. Omit all SUCCESS completions. • TERSE: Trace recording only for FAILING completions; enable extended tracing for FAILUREs. WARNING and SUCCESS completions are not traced. • RESTRICT: Trace recording only for FAILING completions. All extended tracing is disabled. • PREVENT: No recording is performed for HIGH importance events.	VERBOSE	Yes	No

Parameter name	Parameter description	Default value	Update	Output only
ZSRPRIORITYLOWLEVEL	TRACE Z/SERVICE LOW IMPORT TRACE REC. LEVEL Controls the granularity and verbosity of z/Services event recording for lower importance events, but does not exercise control over z/Service Mailbox/PC-call traces. For other events, this parameter can restrict or unfetter ZSR trace recording of events of lesser importance. Low importance events are normally those which relate to the health and execution status of a single Data Virtualization Server transaction of task. Abends in user RPC programs or an authorization failure are examples of low priority events. **ZSRPRIORITYLOWLEVEL** accepts the same values as the **ZSRPRIORITYHIGHLEVEL** start-up parameter. See the discussion there for details on the option settings available and the control each exerts.	NORMAL	Yes	No
ZSRPRIORITYMEDLEVEL	TRACE Z/SERVICE MEDIUM IMPORT TRACE REC. LEVEL Controls the granularity and verbosity of z/Services event recording for MEDIUM importance events. Does not exercise control over z/Service Mailbox/PC-call traces, but for other events, this option can restrict or unfetter ZSR trace recording of MEDIUM importance events. MEDIUM importance events are normally those which control the overall operation and health of Data Virtualization Server. This includes initialization and termination events, abnormal service task terminations, storage usage monitoring, and so on. **ZSRPRIORITYMEDLEVEL** accepts the same values as the **ZSRPRIORITYHIGHLEVEL** start-up parameter. See the discussion there for details on the option settings available and the control each exerts.	VERBOSE	Yes	No

Index

SC27-9811-00