CA XCOM™ Data Transport® for z/OS

Best Practices Guide

Release 11.6

CA Technologies Product References

This document references the following CA products:

- CA Mainframe Software Manager (CA MSM)
- CA XCOM™ Data Transport® for z/OS (CA XCOM Data Transport)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Best Practices Guide Process

These best practices represent years of product experience, much of which is based on customer experience reported through interviews with development, technical support, and technical services. Therefore, many of these best practices are truly a collaborative effort stemming from customer feedback.

To continue and build on this process, we encourage users to share common themes of product use that might benefit other users. Please consider sharing your best practices with us.

To share your best practices, contact us at techpubs@ca.com and preface your email subject line with "Best Practices for *product name*" so that we can easily identify and categorize them.

Contents

Chapter 1: Introduction 7

Purpose of this Guide 7
Audience 7
Mainframe 2.0 Overview 7
Mainframe 2.0 Features 8

Chapter 2: Installation and Configuration Best Practices 11

Installation 11
Configuration for Optimal Performance 12
- Use Maximum Record Packing 12
- Use Large RU Sizes for SNA Sessions 13
- Checkpoint and Restart Considerations 14
- Task Limit Parameters 15
- z/OS Health Checks 16

Data Compression 18
SNA Session Management 20
Secure Sockets Layer (SSL) Usage 21
Hardware Data Encryption Technology 23
KEYRING Access to SSL Certificates 25
Use the PLEXQ Facility to Communicate With Servers 28

Chapter 3: Unicode Transfers Best Practices 29

Network Traffic 29
- Transmission Formats 29
- Considerations 29

Target Datasets 30

Index 31

Chapter 1: Introduction

This section contains the following topics:

Purpose of this Guide (see page 7)
Audience (see page 7)
Mainframe 2.0 Overview (see page 7)
Mainframe 2.0 Features (see page 8)

Purpose of this Guide

The guide provides a brief introduction to the CA Technologies mainframe management strategy and features, and describes the best practices for installing and configuring CA XCOM Data Transport.

Audience

The intended audience of this guide is systems programmers and administrators who install, configure, deploy, and maintain CA XCOM Data Transport.

Mainframe 2.0 Overview

Mainframe 2.0 is our strategy for providing leadership in the mainframe operating environment. We intend to lead the mainframe marketplace for customer experience, Out-Tasking solutions, and solution innovation. After listening to customer needs and requirements to keep the mainframe operating environment viable and cost-effective, we are providing new tools to simplify usage and to energize this operating environment for years to come.

CA Mainframe Software Manager™ (CA MSM) is an important step in realizing the Mainframe 2.0 strategy. CA MSM simplifies and standardizes the delivery, installation, and maintenance of mainframe products on z/OS systems. CA MSM has a browser-based user interface (UI) with a modern look and feel for managing those solutions. As products adopt Mainframe 2.0 features and CA MSM services, you can acquire, install, and manage your software in a common way.

CA MSM provides software acquisition and installation that make it easier for you to obtain and install CA mainframe products, and apply the recommended maintenance. The services within CA MSM enable you to manage your software easily based on industry accepted best practices. The common browser-based UI makes the look and feel of the environment friendly and familiar.

We follow the IBM z/OS packaging standards using SMP/E, with some additional CA qualities of service added, to make installation simple and consistent. Additionally, through the synchronization of product releases and the use of common test environments, we will declare a yearly mainframe software stack that includes many new releases with enhanced functionality. This stack is certified for interoperability across the CA mainframe product portfolio and the base IBM z/OS product stack.

Mainframe 2.0 Features

Mainframe 2.0 has the following main features:

CA Mainframe Software Manager (CA MSM)

Delivers simplified acquisition, installation, and deployment capabilities using a common z/OS-based web application delivered through a browser-based UI. CA MSM includes the following services:

Product Acquisition Service (PAS)

Facilitates the acquisition of our mainframe products and services, including product base installation packages and program temporary fixes (PTFs). This service integrates the inventory of products available on your system with CA Support, providing a seamless environment for managing and downloading software and fixes onto your system.

Software Installation Service (SIS)

Facilitates the installation and maintenance of our mainframe products in the software inventory of the driving system. This service enables you to browse and manage the software inventory using a web interface, and automates tasks for products that use SMP/E to manage installation. You can browse downloaded software packages, and browse and manage one or more consolidated software inventories (CSIs) on the driving system.

Software Deployment Service (SDS)

Facilitates the deployment of CA Technologies mainframe products from the software inventory of the driving system. This service enables you to deploy installed products that are policy-driven with a set of appropriate transport mechanisms across a known topology. The enterprise system topology can include shared DASD environments, networked environments, and z/OS systems. Policies represent a combination of metadata input and user-supplied input. Metadata input identifies the component parts of a product. User-supplied input identifies the deployment criteria, such as where it goes and what it is named.

Electronic Software Delivery (ESD)

Enables you to get our products from an FTP server. We have improved this process so that you no longer need to build a tape to install the product.

Best Practices Management

Integrates with IBM Health Checker for z/OS to verify that deployed software follows our best practices. The health checks continually monitor the system and software to provide feedback on whether the software continues to be configured optimally.

Best Practices Guide

Provides best practices for product installation and configuration.

Note: For additional information about the CA Mainframe 2.0 initiative, see http://ca.com//mainframe2.

Chapter 2: Installation and Configuration Best Practices

This section contains the following topics:

Installation (see page 11)
Configuration for Optimal Performance (see page 12)
Data Compression (see page 18)
SNA Session Management (see page 20)
Secure Sockets Layer (SSL) Usage (see page 21)
Hardware Data Encryption Technology (see page 23)
KEYRING Access to SSL Certificates (see page 25)
Use the PLEXQ Facility to Communicate With Servers (see page 28)

Installation

Use CA MSM to acquire, install, and maintain your product.

Business Value:

CA MSM provides a common way to manage mainframe products. CA MSM provides a web interface, which works with Electronic Software Delivery (ESD) and standardized installation and management of mainframe products. You can use it to download and install CA XCOM Data Transport.

CA MSM lets you download product and maintenance releases over the Internet directly to your system from the CA Support website. After you use CA MSM to download your product or maintenance, you use the same interface to install the downloaded software packages using SMP/E.

Additional Considerations:

After installing the product, use the CA XCOM Data Transport Install Utility to perform the following tasks:

- Set up the product. CA MSM can subsequently be used to maintain your product.
- If there is maintenance, update the VSAM data sets for each region you have set up.

More Information:

For more information about CA MSM, see the *CA Mainframe Software Manager Guide*. For more information about product setup, see the *Installation Guide*.

Configuration for Optimal Performance

The following sections explain the best practices for configuring CA XCOM Data Transport for optimal performance.

Use Maximum Record Packing

Use record packing for most data transfers.

For maximum record packing, use the following parameter values:

- Set the PACK transfer parameter value to YES or LENGTH.

  The PACK parameter causes multiple data records to be placed in the same network buffer.

- Set the MAXPACK parameter in the Default Options Table, or in DEST configuration members for the partners to which the MAXPACK value applies. The MAXPACK value should be set to the largest value allowed (31744).

  The MAXPACK parameter limits the amount of data that will be placed in each buffer.

Business Value:

Packing larger amounts of data in each network buffer reduces the amount of CPU resources required to transfer data.

Additional Considerations:

If your site has network bandwidth constraints or SNA request unit (RU) sizes smaller than the pack buffers, you will have enhanced performance even though you may not benefit from larger network buffer sizes.

Use Large RU Sizes for SNA Sessions

Give careful consideration when defining RU sizes for SNA sessions. RU sizes are analogous to network buffer sizes; larger is usually better.

CA XCOM Data Transport ships the source for a MODETAB, which is a table of LOGMODE entries. LOGMODE entries control the RU size for SNA sessions. You can either assemble and link together the MODETAB as shipped or merge it into your existing MODETAB.

Large RU sizes use less CPU resources than smaller sizes, but require greater bandwidth for effective transmission. If the RU sizes specified for an SNA session are smaller than the PACK buffer, the PACK buffer is split and sent in separate Request Units.

Business Value:

Large RU sizes help to improve network efficiency and conserve CPU resources.

Additional Considerations:

If your site has network bandwidth constraints, you may not benefit from larger RU sizes, but most installations perform better.

Checkpoint and Restart Considerations

Utilize the CA XCOM Data Transport checkpoint and restart feature to reduce the time and resources required to complete interrupted transfers.

Consider the following key factors when setting the CKPT parameter in the Default Options Table, in Destination Members or in individual transfer parameters:

- Set the number of records that can be transferred before a checkpoint is taken.
  - The smaller the CKPT value, the greater the overhead that will be added to what is required to transfer the data.
  - The higher CKPT value reduces the additional checkpoint overhead required to transfer data.
- Set CKPT to a value of zero to disable checkpoint and restart for the file transfers to which the parameter applies.

Notes:

- When transferring PDS data sets, a checkpoint is taken at the end of each member, regardless of the value specified for CKPT.
- If packing is used, the checkpoint taken is based on the number of blocks instead of records processed.

Business Value:

Restarting interrupted transfers from a stored checkpoint lets you complete the transfer without having to restart the transfer from the beginning. This saves you all of the following:

- CPU resources
- Network resources
- Time

Additional Considerations:

Checkpoint and restart performs best when not implemented in a one-size-fits-all manner. Your site will benefit the most from using checkpoint and restart processing in the following situations:

- Volatile or performance constrained network environment
- Very busy or highly competitive DASD I/O configuration
- Very large files to transfer
- Narrow time windows in which the transfers need to complete

Task Limit Parameters

Tune the following task-limiting parameters to levels that will effectively manage the use of system resources by the CA XCOM Data Transport regions:

MAXTASK

Establishes the maximum number of file transfer tasks allowed to be active within the CA XCOM Data Transport region at any given time.

MAXLOC

Establishes the maximum number of locally initiated file transfer tasks allowed to be active within the CA XCOM Data Transport region at any given time.

MAXREM

Establishes the maximum number of remotely initiated file transfer tasks allowed to be active within the CA XCOM Data Transport region at any given time.

Business Value:

Limiting concurrent task levels regulates the amount of system resources that are used by a particular CA XCOM Data Transport region. Tuning CA XCOM Data Transport task levels conserves CPU, virtual storage, I/O activity, and network bandwidth usage for other tasks within the processing environment.

Additional Considerations:

There is no requirement that the value of MAXLOC added to the value of MAXREM must equal MAXTASK.

z/OS Health Checks

Monitor health checks that are generated for CA XCOM Data Transport.

Business Value:

If left uncorrected, Health Checks alert you to conditions that could prevent CA XCOM Data Transport from performing properly. These health checks provide best practices for running CA XCOM Data Transport.

Additional Considerations:

The following health checks are provided for CA XCOM Data Transport:

XCOM_ABOVE_16M@stcname

Storage usage above the 16-MB line is monitored so that CA XCOM Data Transport parameters can be tuned to allow optimized file transfer throughput.

The following two factors most directly impact storage utilization within a CA XCOM Data Transport region:

- Region size
- Values of the MAXTASK, MAXREM, and MAXLOC parameters

XCOM_BELOW_16M@stcname

Storage usage below the 16-MB line is monitored so that CA XCOM Data Transport parameters can be tuned to allow optimized file transfer throughput.

The following two factors most directly impact storage utilization within a CA XCOM Data Transport region:

- Region size
- Values of the MAXTASK, MAXREM, and MAXLOC parameters

XCOM_MAXLOC_LEVEL@stcname

Concurrent locally initiated task levels within the CA XCOM Data Transport region are analyzed against the configured maximum allowed. Percentage utilization is calculated as well as cumulative information about whether the configured maximum number of locally initiated tasks has been reached. During the life of the current server task. The number of times the limit was reached is also displayed.

XCOM_MAXREM_LEVEL@stcname

Concurrent remotely initiated task levels within the CA XCOM Data Transport region are analyzed against the configured maximum allowed. Percentage utilization is calculated as well as cumulative information about whether the configured maximum number of remotely initiated tasks has been reached. During the life of the current server task. The number of times the limit was reached is also displayed.

XCOM_MAXTASK_LEVEL@stcname

Total concurrent task levels within the CA XCOM Data Transport region are analyzed against the configured maximum allowed. Percentage utilization is calculated as well as cumulative information about whether the configured maximum number of tasks has been reached. During the life of the current server task. The number of times the limit was reached is also displayed.

Data Compression

Determine whether data compression provides a performance benefit for file transfers in your particular environment. Environments with limited bandwidth on their networks or where data communications are otherwise constrained benefit most from using data compression. Networks that perform well and have sufficient capacity to process the data traffic to complete file transfers benefit least.

Compressing data is a CPU-intensive task. Different algorithms use different amounts of CPU resources. The primary key to getting performance benefit from using data compression is to balance the amount of CPU used against the percentage by which the size of data buffers is reduced. As a rule, the greater the rate of compression, the greater the amount of CPU required to achieve that rate.

Evaluate and select the appropriate compression algorithm that is the best fit for your processing environment and data content. The allowable values for the COMPRESS= keyword parameter are (presented in ascending order of CPU resource cost):

NO

Disables data compression for the transfers to which this value applies.

YES

Performs basic null and blank compression processing.

RLE

Performs the Run Length Encoding compression method. RLE includes null and blank compression as well as repetitive character compression.

COMPACT

Performs compression that is based on dynamically constructed tables of recurring byte patterns from the compressed data.

HUFFMAN

Performs the Huffman encoding/decoding algorithm for data compression.

ZLIB1 to ZLIB9

Performs ZLIB compression at whatever level is specified. ZLIB1 is the least aggressive (and the least CPU expensive) and ZLIB9 is the top of the scale for both percentage of compression and CPU usage. For backward compatibility, you can specify ZLIB with no numeric qualifier. In this case, the ZLIB keyword is an alias for ZLIB2 compression.

LZRW3

Performs LZRW3 compression, which is a derivative of the Lempel-Ziv family of compression algorithms.

LZSMALL

Performs Lempel-Ziv based compression using the small memory model.

LZMEDIUM

Performs Lempel-Ziv based compression using the medium memory model.

LZLARGE

Performs Lempel-Ziv based compression using the large memory model. Lempel-Ziv is the most stringent data compression method available to CA XCOM Data Transport as well as the most CPU-intensive.

Business Value:

Using data compression can allow existing workloads to be processed while deferring the need for network upgrades, or altogether eliminating the need to upgrade the network.

Additional Considerations:

As mentioned earlier, there is CPU cost for all data compression. It is up to the CA XCOM Data Transport administrator and users to work together to achieve the right balance between the size of transmitted data buffers and CPU usage. This balance varies from one installation to another. Users should be given direction as to which compression methods are most appropriate for any given environment. You can use CA XCOM Data Transport User Exit 7 to screen, and potentially reject, transfer requests that invoke transfer methods disallowed at a particular installation.

The data compression routines that CA XCOM Data Transport uses utilize zIIP processors if available, and ZIIP=YES is specified for the configuration options. zIIP processing reduces the CPU cost of data compression.

SNA Session Management

Evaluate the requirements for handling inactive SNA sessions and select the appropriate option for the DROPSESS= keyword parameter. The valid values for this parameter are detailed, with a description of the functionality of each. The DROPSESS value specified in the CA XCOM Data Transport Default Options applies globally to all SNA sessions within the region. However, this value can be overridden for individual partner LUs by specifying a different value for DROPSESS= in a DEST member that is configured for a specific partner LU.

NO

Causes SNA sessions with partner LUs within the CA XCOM Data Transport server to be retained, even after they are no longer being used.

YES

Causes SNA sessions with partner LUs within the CA XCOM Data Transport server to be terminated at the end of each transfer, without regard to other work that can be pending for the same SNA partner.

QEMPTY

Causes SNA sessions with partner LUs within the CA XCOM Data Transport server to be selectively terminated when there is no more transfer activity queued for a given partner LU.

ALL

Causes all SNA sessions associated with the parallel session connection to a partner to be terminated when there is no more transfer activity queued for a given partner LU.

1 – 60

Specifies the number of minutes that an idle SNA session is retained before being dropped. Using this idle timer method of session management is equivalent to specifying ALL with a timed delay.

Business Value:

Maintaining idle SNA sessions consumes virtual storage within the CA XCOM Data Transport region as well as other system resources associated with keeping a session connected between two LUs. This resource usage is multiplied by the number of sessions that are concurrently active. Reducing the number of idle SNA sessions that are kept active reduces the amount of storage that is required by the CA XCOM Data Transport region while it is in an idle state.

Additional Considerations:

Keeping SNA sessions active can make sense in environments that are CPU constrained, because it eliminates the need to process session establishment for each new request. However, this should be weighed against the cost of holding virtual storage for the duration of each such session.

Secure Sockets Layer (SSL) Usage

Consider deploying Secure Sockets Layer for TCP/IP-based network communications. CA XCOM Data Transport uses OpenSSL as the basis for its data cryptographic services.

The SSL protocol provides data privacy using industry-standard encryption techniques and algorithms. CA XCOM Data Transport's implementation of SSL on the z/OS platform allows for configuring which specific encryption algorithms are used, as well as whether the encryption is performed by software or by hardware via the IBM ICSF interface. The use of certificates for partner authentication is supported.

CA XCOM Data Transport provides scripts for generating certificates and encryption keys which are used for SSL connections. The following is a list of the scripts and their outputs:

makeca

Creates the following data sets:

- random.pem
- certs/cassl.pem
- private/casslkey.pem

Creates the following directories:

- certs
- private

makeclient

Creates the following data sets:

- certs/clientcert.pem
- private/clientkey.pem

makeserver

Creates the following data sets:

- certs/servercert.pem
- private/serverkey.pem

For more information about OpenSSL certificates, see the *CA XCOM Data Transport for z/OS Administration Guide*. All of the CA XCOM Data Transport guides are available on SupportConnect.ca.com if your site is licensed for the product.

Customize the XCOM_SSL_CONFIG data set (typically named configssl.cnf) to the values particular to your installation. This data set must contain the names, path(s) and, optionally, passwords to access your local certificate data sets. This configuration data set also contains options which control whether certificates are validated and which CIPHER algorithms may or may not be used. For more information about configuring your SSL environment for CA XCOM Data Transport, see the *CA XCOM Data Transport for z/OS Administration Guide*.

Business Value:

An organization's data is a valuable asset. Whether the data is in the form of intellectual property or confidential information used in the course of day-to-day operations, maintaining the integrity and privacy of that data is becoming increasingly difficult. Using SSL is an industry-standard means of maintaining this integrity and privacy. Using SSL to protect the transmission of such information allows business operations to be performed while minimizing the risk that the security of sensitive information will be compromised.

Additional Considerations:

Using software-based data encryption is a CPU-intensive operation. This work can be shifted to a hardware function using an IBM cryptographic processor.CA XCOM Data Transport accesses this specialized processor by using the ICSF interface. Using the ICSF interface effectively reduces the amount of general processor resource used to encrypt and decrypt data. This may translate to a cost savings as well due to the reduced number of MSUs that are used in the process of transferring files between systems.

Hardware Data Encryption Technology

If data encryption is desired for CA XCOM Data Transport transfers, this is most efficiently accomplished using the IBM Integrated Cryptographic Service Facility (ICSF). This facility uses a specialized processor and CPU instructions to perform data encryption and decryption using hardware. This stands in contrast to the software-based data encryption provided by OpenSSL. CA XCOM Data Transport supports both OpenSSL and ICSF as tools for encrypting data. Using hardware-based encryption and decryption is more efficient and reduces the amount of general processor resource required to perform secure data transmissions.

For hardware-based encryption, only 3DES is supported.

Several parameter changes must be made in the XCOM_CONFIG_SSL configuration file in order to activate hardware compression support.

Within the [ICSF] section of the XCOM_CONFIG_SSL data set, the following parameters need to be set:

INITIATE_SIDE=CLEAR | NO

Applies to cases when this XCOM is the client (local machine)

RECEIVE_SIDE=CLEAR | NO

Applies to cases when this XCOM is the server (remote machine).

The allowable values and associated functionality for these parameters are:

CLEAR

Stores the symmetric keys in clear text in memory during the transfer and uses the ICSF CSNBSYE/CSNBSYD encryption functions.

NO (default)

Uses the OpenSSL software encryption routine.

You also need to disable AES encryption in the configuration data set, because it will always invoke OpenSSL encryption. Disabling AES encryption is also done in the XCOM_CONFIG_SSL file, using the ! character. The following example of keyword values will accomplish this:

```
[CIPHER]
INITIATE_SIDE = ALL:!AES:!ADH:!LOW:!EXP:MD5:@STRENGTH
RECEIVE_SIDE = ALL:!AES:!ADH:!LOW:!EXP:!MD5:@STRENGTH
```

Business Value:

Using less general processor resource translates to cost savings. It may directly result in reduced billable CPU usage or free up processor resources for other tasks within the system. Another possible benefit is to defer or eliminate the need to upgrade or add general processor capacity.

Additional Considerations:

Consult your IBM representative for availability and pricing of the ICSF feature for your specific processing environment.

KEYRING Access to SSL Certificates

Consider loading the certificates used for SSL connections into your external security manager software.

Business Value:

Many external security manager software packages provide a facility by which certificates can be stored and retrieved easily for use based on the USERID associated with the connection or file transfer. These certificate storage locations are called KEYRINGs. Placing certificates within a security manager software package KEYRING provides additional environmental security by controlling which certificates get selected for use by CA XCOM Data Transport activities. This prevents undesired or unauthorized changes to stored certificate content as well as the usage of unapproved certificates.

Additional Considerations:

An additional benefit to maintaining certificates in a managed KEYRING is a reduction in required ongoing maintenance of configuration data sets used by CA XCOM Data Transport, because the certificate information is made accessible through a call to the security management software.

To place certificates in a KEYRING

1. Use the following commands to export both the client and the server certificates to a format suitable for loading into a KEYRING:

   Client

   ```
   Openssl 12 –export –in </path/client.pem> –inkey </path/clientkey.pem> –certfile
   </path/cassl.pem> –name <“Client”> –out <client.p12>
   ```

   Server

   ```
   Openssl pkcs12 –export –in </path/server.pem> –inkey </path/serverkey.pem>
   –certfile </path/cassl.pem> –name <“Server”> –out <server.p12>
   ```

   Explanation of parameters:

   </path/client.pem> or </path/server.pem>

   Indicates the name of the server and client certificate files and the path where they can be found. The path is not needed if you are executing the command from the same directory where these files reside.

   </path/clientkey.pem> or </path/serverkey.pem>

   Indicates the name of the server and client key files and the path where they can be found. The path is not needed if you are executing the command from the same directory where these files reside.

</path/cassl.pem>

Indicates the name of the CA certificate file and path where it can be found. The path is not needed if you are executing the command from the same directory where this file resides.

-name <"Client"> or –name <"Server">

A descriptive name associated with the client or server certificate.

-out <client.p12> or –server <server.p12>

The name of the output file that will contain the PKCS12 formatted version of the client and server certificates.

2. Create three sequential DSORG=PS and RECFM=VB data sets, and then catalog them on your system.

   One is needed for the CA certificate, one for the client certificate, and one for the server certificate.

3. Copy the certificates created in Step 1 to the data sets created in Step 2, as follows:

   - cassl.pem (CA certificate) to the CA data set
   - The <server.p12> file to the server data set
   - The <client.p12> file to the client data set

   Note: Because these files reside on an HFS directory, you can use either TSO ISH or FTP to copy them to the data sets created in Step 2. If using TSO ISH, then ensure a binary copy is done for the converted server and client files so that no conversions occur with the data. The CA file can do just a straight ASCII copy.

4. Add the certificates to the external security manager software. Please consult the documentation for your security software to determine the appropriate procedures and commands to use to add the exported certificates to your security software.

5. Define the KEYRING and LABLCERT names to which you have assigned your certificates in your external security software. The following are the keywords that are used in your XCOM_CONFIG_SSL data set to accomplish this. The KEYRING and LABLCERT values are used to uniquely identify the particular set of certificates that are to be retrieved and used for your SSL connection with the partner system.

   In the [KEYRING] section of the XCOM_CONFIG_SSL data set, the following parameters need to be set:

   INITIATE_SIDE = <keyring name>

   Applies to cases when this XCOM is the client (local machine).

RECEIVE_SIDE = <keyring name>

Applies to cases when this XCOM is the server (remote machine).

In the [LABLCERT] section of the XCOM_CONFIG_SSL data set, the following parameters need to be set:

INITIATE_SIDE = <lablcert name>

Applies to cases when this XCOM is the client (local machine).

RECEIVE_SIDE = <lablcert name>

Applies to cases when this XCOM is the server (remote machine).

Use the PLEXQ Facility to Communicate With Servers

Consider using the PLEXQ facility for communication with CA XCOM servers from the XCOMJOB batch requests instead of SNA or TCP/IP protocols.

If a group name is specified on the PLEXQ parameter in the CA XCOM CONFIG member, a CA XCOM server becomes PLEXQ enabled. The PLEXQ facility uses SYSPLEX Signaling Services to communicate between CA XCOM address spaces. No advance or separate system configuration is required to connect a CA XCOM server to a PLEXQ group.

XCOMJOB can communicate with a single server, or group of servers which are joined to the same PLEXQ group. The STCPLEXQ EXEC PARM for XCOMJOB designates which PLEXQ group is to receive the request from XCOMJOB. (STCPLEXQ is mutually exclusive with the STCAPPL and STCIP parameters.)

If a single server is connected to PLEXQ XCOM1, executing XCOMJOB TYPE=SCHEDULE with STCPLEXQ=XCOM1 parameter directs the request to the server connected to XCOM1.

If multiple servers are connected to the PLEXQ group XCOM1, the transfer is scheduled to the best candidate to receive the schedule request. This functions in a manner similar to the current XCOMPLEX facility. Thus, the PLEXQ facility ultimately replaces XCOMPLEX functions.

A TYPE=HISTORY request to a PLEXQ group of servers retrieves matching history records from ALL of the servers which are connected to the PLEXQ group. A TYPE=INQUIRE request is directed to the specific server to which the transfer was previously scheduled.

Business Value:

The PLEXQ facility provides a more efficient means to communicate with CA XCOM servers than previously required protocols. PLEXQ can also provide functionality found in an XCOMPLEX configuration. However, with PLEXQ, there is no need for an ADMIN server. PLEXQ communication between CA XCOM address spaces requires a reduced amount of system resources then conventional protocols.

Additional Considerations:

PLEXQ functionality can be implemented alongside XCOMPLEX environments to allow for migration to the new technology. The XCOMPLEX feature is being deprecated, and is eventually removed from the product.

Chapter 3: Unicode Transfers Best Practices

This section contains the following topics:

Network Traffic (see page 29)
Target Datasets (see page 30)

Network Traffic

When transmitting data between partners in a Unicode format (UTF-8 or UTF-16), it is important to understand what type of data is being transmitted as not to cause more network overhead. Depending on the type of data is being transmitted, there could be a significant difference in the amount of data that is sent over the network that is between the two formats.

Transmission Formats

UTF-8 Format – a single character is encoded in a 1- to 4-byte format. The first 128 characters of UTF-8 correspond to the ASCII character set.

UTF-16 Format – a single character is encoded in a 2-byte format. For characters outside of the basic multilingual plane, 4 bytes would be required.

Considerations

For data that is comprised mostly of single-byte characters (SBCS), using the UTF-8 format for transmission would yield the least amount of data transmitted. The translation to UTF-8 would be mostly a 1-1 correspondence in bytes per character, where UTF-16 would use 2 bytes per character.

For data comprised of mostly double byte characters (DBCS), using the UTF-16 format for transmission would yield the least amount of data transmitted. The translation to UTF-16 would be 2 bytes per character, where UTF-8 has the potential to use more than 2 bytes per character.

Target Datasets

When defining a target dataset, the following considerations are used to determine the logical record length (LRECL) to use:

- Logical record length of the source dataset
- Character set that the source dataset uses
- Character set to be used for the target dataset

When going from a single byte character set (SBCS) to a double (DBCS) or multibyte (MBCS) character set, the LRECL of the target dataset would need to be larger than the source. This is to account for the DBCS and MBCS characters taking more than a single byte for storage. For example, when going from a single byte character set to a double byte character set, the LRECL of the target dataset should be at least double the source dataset, since DBCS characters take up 2 bytes of storage.

In cases where there are mixed character sets within the data, a variable length record definition would also allow for conservation of the disk space.

Index

A

acquire the product • 11

C

CKPT parameter • 14
compression • 18
configuration options • 12

D

data compression • 18
DROPSESS parameter • 20

E

encryption • 23

H

health checks • 16

I

ICSF • 23
install utility • 11
interrupted transfers, restarting • 14

K

KEYRING access • 25

L

LOGMODE entries • 13

M

Mainframe 2.0
  components • 8
  overview • 7
MAXLOC parameter • 15
MAXPACK parameter • 12
MAXREM parameter • 15
MAXTASK parameter • 15

P

PACK parameter • 12
parameters
  for limiting tasks • 15
  for record packing • 12
PDS data set transfer checkpoints • 14
performance configurations • 12

R

record packing for data transfers • 12

S

SNA RU sizes • 13
SNA sessions • 20
SSL • 21, 25

T

TCP/IP • 21, 25
transfer parameters • 12, 14, 15

X

XCOM_CONFIG_SSL parameter • 21