CA NetMaster® File Transfer Management

Best Practices Guide

r12

CA Product References

This document references the following CA products:

- CA NetMaster® File Transfer Management (CA NetMaster FTM)

- CA NetMaster® Network Automation (CA NetMaster NA)

- CA NetMaster® Network Management for SNA (CA NetMaster NM for SNA)

- CA NetMaster® Network Management for TCP/IP (CA NetMaster NM for TCP/IP)

- CA OPS/MVS® Event Management and Automation (CA OPS/MVS)

- CA XCOM™ Data Transport®

Contact CA

Contact Technical Support

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

- 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

Provide Feedback

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

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found 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

This section contains the following topics:

Purpose of this Guide

The guide provides a brief introduction to CA's Mainframe 2.0 strategy and features, and describes the best practices for installing and configuring CA NetMaster FTM.

Audience

The intended audience of this guide is systems programmers and administrators who install, configure, deploy, and maintain CA NetMaster FTM.

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 our 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 CA metadata input that identifies the component parts of a product and user-supplied input that identifies the deployment criteria, such as where it will go and what will it be called.

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

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

Business Value:

CA MSM provides a web interface, which works with ESD and standardized installation, to provide a common way to manage CA mainframe products. You can use it to download and install CA NetMaster FTM.

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 you install the product, use the product's Install Utility to set it up. CA MSM can continue to help you maintain your product.

Note: If there is maintenance for VSAM data sets, you must use the Install Utility to update those data sets for each region you have set up.

More Information:

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

Address Space Sharing

If your site also uses CA SOLVE:FTS, share the address space with CA SOLVE:FTS for performance and usability optimization. To share the address space, set up a region that includes the products.

CA NetMaster FTM can also share address space with the following products:

- CA NetMaster NM for TCP/IP
- CA NetMaster NM for SNA
- CA NetMaster NA

Business Value:

Sharing an address space has the following values:

- You require only a single logon to access multiple products from one interface.
- You have better integration between products. You can have a single integrated configured address space instead of having to configure multiple address spaces.
- The multiple products can share resources.

Security Considerations

Implement the NMSAF solution. The NMSAF solution is built around a partial security exit. The solution uses the product's User Access Maintenance Subsystem (UAMS) data set to store information for your product region, and uses your installed security product to perform user validation and password checking (through the IBM-defined system authorization facility (SAF) interfaces).

Business Value:

This setup is ideal for organizations that want the flexibility of allowing the administrator to control specific region authorities, while still ensuring that access to the region is secured by their security product.

More Information:

For more information about the NMSAF solution and UAMS, see the *Security Guide*.

Background Users

In a multisystem environment, reduce the number of background user IDs you add to security by specifying the same value for NMSUP in all regions.

Business Value:

Particularly in large complexes, this practice assists in simplifying the administration of internal background user IDs and reduces the possibility of outages associated with nonexistent, or incorrectly defined user IDs.

Additional Considerations:

CA NetMaster FTM uses background users to perform various tasks. By default, the NMSAF solution checks the background user IDs in advanced program-to-program communications (APPC). You must add them to your installed security product.

Note: The following NMSAF SXCTL parameters set the user ID checking: APPCCHECK and SYSCHECK.

The following list identifies the background user IDs:

- *xxxx*AOMP

- *xxxx*BLOG

- *xxxx*BMON

- *xxxx*BSVR

- *xxxx*BSYS

- *xxxx*LOGP

xxxx

Is the prefix specified by the NMSUP region job control language (JCL) parameter.

By specifying the same value for NMSUP in all regions, you only have to add one background user to security. For example, if you set NMSUP to MFNM in all regions, then the user ID for the *xxxx*BSYS background users in those regions is MFNMBSYS.

To use NMSUP, add the following statement to the TESTEXEC(RUNSYSIN) members for the regions, using the same *xxxx* value:

PPREF='NMSUP=*xxxx*'

More Information:

For information about SXCTL, see the *Security Guide*.

Configuration for Optimal Performance

As a performance pattern develops for your product, tune the relevant controls. You probably never have to tune many of the controls.

Business Value:

Reviewing the configuration and tuning parameters helps ensure that you are not performing unnecessary processing, such as collecting and logging data that your organization does not require, thus saving CPU cycles. As you become more familiar with the capabilities of the product, you can make informed decisions on what functions are desirable and therefore only incur overhead where there are obvious benefits.

Additional Considerations:

A product with the breadth and capability of CA NetMaster FTM supports many external tuning controls. Configuring every last aspect of its operation can seem like a large task. However, you can set up an effective environment by simply using the default settings.

If you have a newly implemented region, a basic configuration is created with some essential parameters updated during setup. Further customization can be performed progressively.

More Information:

For more information about product setup and initial startup, see the *Installation Guide*.

zIIPs

If IBM System z Integrated Information Processors (zIIPs) are available, elect to use zIIPs when you set up your regions.

Business Value:

Using zIIPs provides the following benefits:

- Reducing the execution time on the normal central processing unit (CPU), providing savings in billable CPU time
- Freeing up processing cycles from the CPU to other work
- Exploiting the processing power of zIIPs

More Information:

The following JCL parameters control the usage of zIIPs: PAEXMODE for the SOLVE Subsystem Interface and XM for the region. For information about the parameters, see the *SOLVE Subsystem Interface Guide* and *the Reference Guide*.

Standardized Object Naming

Name resources in a standard way.

Business Value:

Presentation, management, and control of CA NetMaster FTM objects (resources, rule sets, and rules) is better when objects are organized and named in a structured and standard way. A naming standard makes the product easier to use (less training with less user error). Additionally, generic automation is easier when dealing with objects that conform to a standard, reducing the effort and maintenance required for building automation.

Example: EventView Rule Set Names

In EventView, you can implement multiple rule sets and include them in a primary rule set. The following naming organizes the rule sets in a structured way. The standard uses the first part of the name to identify the type of resource and the second part of the name to identify the rule action. For example, the CICSAUTO rule set automates actions in response to CICS messages, the FTENH rule set enhances the presentation of file transfer messages, and the ZOSSUPP suppresses z/OS messages.

```
PRIMARY
     CICSAUTO
     CICSEHN
     CICSSUPP
     FTAUTO
     FTENH
     FTSUPP
     ZOSAUTO
     ZOSENH
     ZOSSUPP
```

Automation for File Transfer Schedule Monitors

Use the Additional Details panel of an FTSCHD-class file transfer schedule monitor resource when automating schedule activities.

Business Value:

CA NetMaster FTM encourages the automation of manual processes. Coding of automation is expensive in terms of time, effort, and maintenance when point solutions are developed. The Additional Details panel stores specified text as variables that you can use in a generic process. Building automation using generic processes enables one piece of automation code to be used for multiple resources.

Additional Considerations:

The definition for a file transfer schedule monitor resource includes an Additional Details panel, where you can add 16 lines of free-format text. Values entered at this panel are available to processes as variables, &ZRMDBADDET1 through &ZRMDBADDET16. Each line can hold 70 characters of text. The Additional Details panel supplements other panels whereby resource data is made available to automation processing.

Monitoring of file transfer schedules is often closely related to batch processing. A good use of this panel would be to standardize areas of this panel for use in building generic automation for batch processing, for example:

- Use Line 1 to specify the prerequisite suite of batch jobs.

- Use Line 2 to specify the contact details (for example, name and telephone number) for the prerequisite jobs.

- Use Line 3 to specify the post-processing suite of batch jobs.

- Use Line 4 to specify the contact details for the post-processing jobs.

Your automation process can use &ZRMDBADDET1through &ZRMDBADDET4 to ascertain batch processing details, and you can define one generic process to manage all file transfer schedules.

More Information:

For more information about how to define processes, see the *Administration Guide*.

Transient Logs

Tune your transient logs to reduce storage. Disable all logging initially, and then implement logging for business critical resources (applications).

Business Value:

Mainframe storage costs money and should be used only if there is a business requirement. Tuning the size of transient logs enables you to set storage at a level appropriate to your business requirements.

Additional Considerations:

Transient logs provide a snapshot history of activities at the resource level. From a resource monitor, you can use the SETTLOG command to disable logging or reset the log size for one or more monitored resources.

Online Help

Use online help to find out more about the interface in context.

Business Value:

CA NetMaster FTM has many features and can be overwhelming to new users. However, you have access to substantial online help at both the 3270 and WebCenter interfaces, usually by pressing F1 or clicking the Help link. You are encouraged to request online help, to promote product understanding, save time on issue resolution, and potentially save money on basic product training.

Interfaces and Integration Points

Integrate with other CA products to help you manage your business.
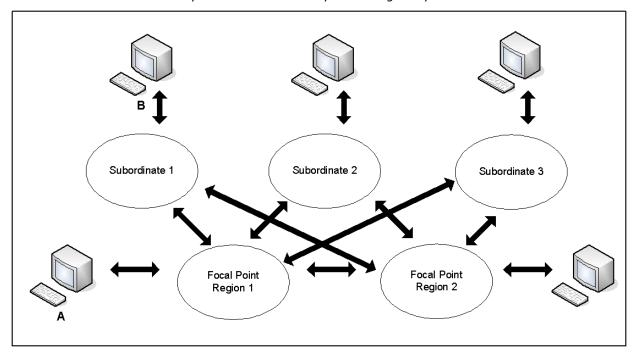
Business Value:

CA NetMaster FTM integrates with the following CA products:

- **Other CA NetMaster products**—All CA NetMaster products can share the same address space. They can also communicate with each other using their multisystem capabilities. The use of common monitors, such as the alert monitor and the status monitor, supports the monitoring and control of network events and resources irrespective of whether they are IP, SNA, or file transfer related.

- **CA XCOM Data Transport**—CA NetMaster FTM supports the monitoring of CA XCOM Data Transport transfers either originating or ending on z/OS. You can define service windows to monitor these transfers, enabling issues to be quickly identified and resolved before they affect your business.

- **CA SOLVE:FTS**—CA NetMaster FTM supports the monitoring of CA SOLVE:FTS transfers. You can define service windows to monitor these transfers, enabling issues to be quickly identified and resolved before they affect your business.

- **CA Service Desk**—CA NetMaster FTM supports the automatic creation of trouble tickets in CA Service Desk, facilitating problem notification and resolution.

- **CA OPS/MVS**—CA OPS/MVS can forward system events programmatically to CA NetMaster FTM for display on the alert monitor. The monitor is an ideal consolidation point for all mainframe network and system events. The integration facilitates the flow of information between CA management products and users.

Multisystem Deployment

If you have multiple systems, deploy CA NetMaster FTM in a multisystem environment to provide a consolidated view of your enterprise.

The following diagram shows an example of a multisystem environment. Logging on to Console A allows visibility to all resources. Logging on to Console B allows visibility to the subordinate system image only.

Business Value:

Particularly in large multisystem environments, deployment can be both arduous and time consuming. Following an effective and proven process has the following values:

■   Reduce the time taken to migrate to new releases, and therefore enable access to new functions more readily.

■   Free key resources to perform other tasks, such as the exploitation of product functions.

■   Reduce the likelihood of errors and subsequent outages associated with poor deployment processes.

Additional Considerations:

We recommend that you use the CA MSM SDS to deploy the product SMP/E target libraries to the remote systems.

Note: For more information about SDS, see the *CA Mainframe Software Manager Product Guide*.

You set up and configure the product once, typically on a test system, which becomes the deployment system. After the product is configured, you create a backup data set for the configuration files (see page 26). You can then use SDS to deploy the product target libraries and at the same time, the backup data set as a custom data set. On the remote system, you can restore the configuration files from the deployed backup data set.

How Deployment Works

Before you proceed to perform multisystem deployment, you should have one properly configured region.

Typically, deployment consists of the following stages:

1. Create a generic RUNSYSIN member and a generic initialization file for sharing between regions.

2. Copy the required data sets to and allocate them on the target systems.

3. Deploy started task members on target systems.

4. APF authorize load libraries on target systems.

5. Determine focal and subordinate regions.

6. Link regions to create the multisystem environment.

More information:

Software Changes

Changes are required to set up subsystem IDs, load libraries, and VTAM:

- Subsystem IDs are required for the initialization of the required subsystems. The IDs have the following default values:
    - SOLV for the SOLVE Subsystem Interface (SSI), which enables a region to communicate with other software on the system
    - Domain ID of the region for the region interface that enables a region to issue operating system commands and receive messages
    - (Optional) NFTP for the NMFTP Monitor, which enables a region to monitor FTP events on an IBM TCP/IP stack

    The SOLVE SSI started task, the region, and the NMFTP started task automatically identify these IDs to the system. If you want to set the IDs permanently, you can set them in the SYS1.PARMLIB(IEFSSN*xx*) member. Add the ID for the region interface first (after the job entry subsystem (JES)) in the list of subsystem names.

- The following load libraries for CA NetMaster FTM must be APF-authorized:
    - CC2DLOAD
    - CC22DPLD (If SSL is installed)

- A VTAM major node member, which contains application definition statements for all ACBs required by your product region, must be created and added to SYS1.VTAMLST. You can use the Create VTAM Definitions and Table option of the product's Install Utility to perform this task.

Note: For more information, see the *Installation Guide*.

Create Generic Initialization File and RUNSYSIN Member for Multiple Regions

Create a generic RUNSYSIN member that points to a generic initialization file so you can use the member for all the regions deployed in your enterprise.

To create generic initialization file and RUNSYSIN member

1. Generate the initialization file for a properly configured region.

2. Replace specific information in the file by product variables and system symbols.

   A generic initialization file is created.

3. Replace specific information in RUNSYSIN by system symbols.

4. Update RUNSYSIN with the following statement:

   `PPREF='INIFILE=`*xxxx*`INI'`

   ***xxxx*INI**

   > Is the name of the generic initialization file.

   A generic RUNSYSIN member is created.

5. Start the region using the generic RUNSYSIN member to verify that it is free of errors.

   If initialization errors occur, review RUNSYSIN and the initialization file to correct the errors.

6. Repeat the previous step until the region initializes without error.

   The generic RUNSYSIN member is ready for use by other regions.

Region Initialization File

Region customization parameters are stored in a virtual file system (VFS) data set, which is a virtual storage access method (VSAM) data set and is not easy to update outside of CA NetMaster FTM. However, a RUNSYSIN member can point to an initialization file member in TESTEXEC by using the INIFILE parameter.

An initialization file is a Network Control Language (NCL) procedure that contains the parameter information.

When an initialization file is in use, the region gets the parameter information from the file at startup and updates the VFS data set. Because the region uses the initialization file each time it starts up, any changes you make manually using the /PARMS panel shortcut are not retained. To keep the changes, regenerate the file using the /CUSTOM.G panel path.

Even if you do not use the initialization file for region startup, you can use it as a backup of the parameters in the VFS data set by generating it before updating the parameters using /PARMS.

The initialization file is also useful during rollout to other systems because it is relatively simple to update for different systems. Through the use of product variables and system symbols, the file can be made generic enough for all the regions you plan to deploy.

Note: For more information about how to use a region initialization file, see the *Administration Guide*.

Generic Initialization File

You can modify an initialization file to use system symbols to support its use throughout your enterprise.

Example: Initialization File With System Symbols

The following sample code shows statements for the LOGFILES parameter group using the &SYSNAME system symbol:

```
.LOGFILES
    &$IAPLOGPR    = &STR $LOPROC
    &$IAPLOGVW    = &STR $LOBROW
    &$IAPLOGF1    = &STR NMLOG01
    &$IAPLOGD1    = &STR NETW.NM.NETM&SYSNAME.NMLOG01
    &$IAPLOG01    = &STR LSR SIS DEFER
    &$IAPLOGI1    = &STR SHR
    &$IAPLOGF2    = &STR NMLOG02
    &$IAPLOGD2    = &STR NETW.NM.NETM&SYSNAME.NMLOG02
    &$IAPLOG02    = &STR LSR SIS DEFER
    &$IAPLOGI2    = &STR SHR
    &$IAPLOGF3    = &STR NMLOG03
    &$IAPLOGD3    = &STR NETW.NM.NETM&SYSNAME.NMLOG03
    &$IAPLOG03    = &STR LSR SIS DEFER
    &$IAPLOGI3    = &STR SHR
```

Generic RUNSYSIN

By building a RUNSYSIN member using system symbols, you can create a generic RUNSYSIN member that can be deployed throughout your enterprise.

You can identify the symbols defined to your system from the response to the following system command:

```
D SYMBOLS
```

To tell the NETMASTR program to perform symbol substitution, include the following statement in RUNSYSIN:

```
SUBS=YES
```

Example: RUNSYSIN With System Symbols

The following sample code shows RUNSYSIN statements using the &SYSNAME and &SYSCLONE system symbols:

```
SUBS=YES -* Required to invoke system symbols
PGM=NM001
ERROR=U0001
PPREF='PRI=NETM&SYSNAME' -* if &SYSNAME = "ABCD", PRI=NETMABCD
PPREF='NMDID=&SYSCLONE.NW'
PPREF='INIT=NMINIT'
PPREF='READY=NMREADY'
PPREF='SSID=NMSS'
PPREF='DSNQLCL=NETW.NM.NETM&SYSNAME'
PPREF='DSNQLNV=NETW.NM.VSAM.NETM&SYSNAME'
```

Note: A symbol used in the middle of the name must be defined with two periods (..), for example:

```
DD=VFS,DISP=SHR,DSN=NETW.NM.NETM&SYSNAME..VFS
```

Data Set Deployment

During deployment, you copy the following data sets to the target systems. However, in a shared DASD environment, you do not need to copy those data sets that are marked as shareable.

Note: When deploying CA NetMaster FTM with other CA NetMaster products, such as CA NetMaster NM for SNA, additional data sets specific to these products may also be required. For information, see the *Best Practices Guide* specific to those products.

You must copy the following data sets:

- ALERTH
- EVNTDB
- EVNTSEQ
- FTLOG01
- FTLOG02
- FTLOG03
- ICOPANL
- MODSUSR
- NMLOG01
- NMLOG02
- NMLOG03
- OBEYFILE
- PANLUSR
- PSPOOL
- RAMDB
- RAMDBST
- RAMDBWK
- REXXAN
- REXXREP
- TESTEXEC
- VFS

The following data sets can be shared:

- CC11EXEC (shareable)

- CC17EXEC (shareable)

- CC2DEXEC (shareable)

- CC2DLOAD (shareable)

- CC2DPLD (shareable)

- MODSDIS (shareable)

- OSCNTL (shareable)

- PANLDIS (shareable)

- PARMLIB (shareable)

- SSIPARM (shareable)

- UAMS (shareable)

One method to distribute data sets is to use a backup utility, such as DFDSS, to create a single data set that can be transferred to the target systems and restored.

When the Install Utility sets up a region, the utility creates the following data set members:

S10DUMP

Creates a backup data set that includes the configuration files for the region.

S11REST

Restores the configuration files from the backup data set.

After you submit the S10DUMP job, you use SDS to deploy the created backup data set to the target system. Also, you copy the S11REST job to the target system. On the target system, you submit S11REST to restore the configuration files.

Started Task Deployment

During deployment, you copy the region and SOLVE SSI started task members to SYS*x*.PROCLIB on the target systems.

Software Changes on Target Systems

During deployment, you add the subsystem IDs and ACBs, and APF-authorize the load libraries on the target systems.

Multisystem Configuration

Regions can be linked together into a complex. Within a complex, you can have two types of regions: focal and subordinate.

A focal region has visibility to, and command and control capabilities over, every region in the complex, including other focal regions.

A subordinate region only sends data to the focal regions. A subordinate does not receive data from other regions in the complex.

To reduce network traffic, focal regions only receive status information if someone is actually using one of the various monitors.

In a multisystem environment, operators can log on to one focal region and monitor the entire complex.

The Resource Automation Monitor database (RAMDB) for a focal region contains copies of the system images for all regions within the complex. The RAMDB for a subordinate region contains only the system images for itself.

In general, you configure regions on communication management configuration (CMC) systems (hosts) as focal, and all the others as subordinate.

How You Prepare RAMDB Before Linking

You can use the following methods to prepare RAMDB before you link your regions to set up the multisystem environment:

Important! When you link two regions, one region has the database you want and the other region will have its database overwritten. Linking must always be initiated from the region whose database is to be overwritten.

■ You can create the system images for the individual systems on which the regions are deployed. You then assign one region as focal, transmit the images from the other regions to it, and then link the other region to it.

The linking must be done from the new region where the database is deleted and rebuilt to mirror that in the focal region.

■ You can create the system images for all the required systems in the complex in the main focal region. Then each new region can be deployed with the default RAMDB provided during setup. The default RAMDB is deleted and rebuilt with the required system images when the region is linked to the focal region.

After the regions are linked, their RAMDBs are kept synchronized automatically.

Note: For more information about how to set up a multisystem environment, see the *Administration Guide*.

Index

A

automation • 16

B

background users • 13

C

CA MSM (CA Mainframe Software Manager) • 8, 11
configuration • 14

D

data sets, deployment • 26
deployment • 19

E

ESD (Electronic Software Delivery) • 8

F

file transfer scheule monitors • 16

H

health checks • 8
help • 17

I

initialization • 22
installation • 8
integration • 18

M

Mainframe 2.0 • 7
multisystem support • 19

N

naming of objects • 15
NMFTP Monitor • 21

O

object naming • 15
offloading work from • 14
online help • 17

P

PAS (Product Acquisition Service) • 8

R

RAMDB • 28

S

SDS (Software Deployment Service) • 8
security • 12
setup • 12
sharing • 12
SIS (Software Installation Service) • 8
size, transient logs • 17
SOLVE SSI • 21

T

transient logs • 17

Z

zIIPs • 14