

CA NetMaster® Network Management for TCP/IP

Installation Guide

Release 12.1



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2012 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Application Performance Management (CA APM)
- CA Cross-Enterprise Application Performance Management (CA Cross-Enterprise APM)
- CA Introscope® (CA Introscope)
- CA NetMaster® Network Management for TCP/IP (CA NetMaster NM for TCP/IP)
- CA NetMaster® File Transfer Management (CA NetMaster FTM)
- CA NetMaster® Network Management for SNA (CA NetMaster NM for SNA)
- CA NetMaster® Network Automation (CA NetMaster NA)
- CA SOLVE:FTS
- CA NetSpy™ Network Performance (CA NetSpy)
- CA SOLVE:Operations® Automation
- CA SOLVE:Access™ Session Management (CA SOLVE:Access)
- CA Network and Systems Management NetMaster® Option (CA NSM NetMaster Option)
- CA Network and Systems Management (Unicenter NSM)
- CA NetMaster® Socket Management for CICS (CA NetMaster SM for CICS)
- CA Common Services for z/OS
- CA Common Inventory Service
- CA Auditor for z/OS (CA Auditor)
- CA TCPaccess™ Communications Server for z/OS (CA TCPaccess CS)
- CA TCPaccess™ Telnet Server (CA TCPaccess Telnet Server)
- CA ACF2™ for z/OS
- CA Top Secret® for z/OS
- CA SYSVIEW® Performance Management (CA SYSVIEW)

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>.

Contents

Chapter 1: Overview 11

Audience	11
How the Installation Process Works.....	11

Chapter 2: Preparing for Installation 13

Multiple Product Installation and Setup	13
Software Requirements	13
Operating Environment.....	13
WebCenter Requirements	14
Migration Mode	14
CA Common Services Requirements	15
Security Requirements	16
Storage Requirements.....	17
How CA LMP Statements Are Coded.....	17
KEYS Member—Add Execution Key	17
CA LMP Key Certificate.....	19
Worksheets	20
Migration Preparation.....	20
Parameter Group Values.....	20
How to Migrate Your Initialization File	21
Knowledge Base	21
Multisystem Considerations	21

Chapter 3: Installing Your Product Using CA MSM 25

How to Use CA MSM: Scenarios.....	26
How to Acquire a Product	26
How to Install a Product.....	27
How to Maintain Existing Products	29
How to Set Up the System Registry	30
How to Deploy a Product	32
How to Configure a Product.....	33
Access CA MSM Using the Web-Based Interface	34

Chapter 4: Installing Your Product from Pax-Enhanced ESD 37

How to Install a Product Using Pax-Enhanced ESD	37
---	----

How the Pax-Enhanced ESD Download Works	39
ESD Product Download Window	39
USS Environment Setup	42
Allocate and Mount a File System	43
Copy the Product Pax Files into Your USS Directory	46
Download Using Batch JCL	47
Download Files to Mainframe through a PC	50
Create a Product Directory from the Pax File	51
Sample Job to Execute the Pax Command (Unpackage.txt)	52
Copy Installation Files to z/OS Data Sets	52
Unload the Install Utility	53
Additional Features	54
Installation JCL	54
Generate the Installation JCL	55
Clean Up the USS Directory	57
Maintenance	58
Product Maintenance	58
Apply Maintenance	59
Update VSAM Data Sets	63
Individual RAMDB Maintenance	64

Chapter 5: Installing Your Product from Tape 71

Unload the Install Utility	71
Additional Features	71
Unload into a New Data Set from Tape	71
Unload into an Existing Data Set from Tape	73
Installation JCL	74
Generate the Installation JCL	74
Maintenance	77
Product Maintenance	77
Apply Maintenance	77
Update VSAM Data Sets	81
Individual RAMDB Maintenance	83

Chapter 6: Configuring Your Product 89

How Region Setup Works	89
Region Contents	89
SOLVE SSI as Common Component	90
Specify the SOLVE SSI Region	90
Specify the Product Region	92

Chapter 7: Creating VTAM Definitions and Tables **95**

Create VTAM Definitions and Tables	95
--	----

Chapter 8: Preparing the IBM Communications Server **97**

Review Your SOLVE SSI Configuration	97
Set Up the SNMP Agent	98
SMF Record Creation.....	99
Generate SMF Records.....	99
Define UNIX Authorization for Your Started Task User IDs	101
Authorize SOLVE SSI Command Access	101
Example: Authorization in a CA ACF2 System that Protects Operator Commands	101
Example: Authorization in a CA Top Secret System	101
Example: Authorization in a RACF System	101
SNA Network Management Interface Setup	102
SNA Network Management Interface Security Requirements	102
IPSec Network Management Interface Setup	103
IPSec Network Management Interface Security Requirements	104
Authorize Product Region Command Access	106
Example: Authorization in a CA ACF2 System that Protects Operator Commands	106
Example: Authorization in a CA Top Secret System	106
Example: Authorization in a RACF System	106
User Authorization to View Packet Payload Data	107
CA Top Secret	107
CA ACF2	107
RACF	108
User Authorization for IP Security Functions	108

Chapter 9: Preparing CA TCPaccess Telnet Server **109**

Enable Event Interface	109
Define the Server Exit.....	109
Generate SMF Records.....	110
Restart CA TCPaccess	110

Chapter 10: Preparing CA TCPaccess CS **111**

Enable Event Interface	111
Define the Server Exit.....	112
Generate SMF Records.....	112
Set Up DNR Members	113
Enable Access to SNMP Data.....	113

Restart CA TCPaccess	114
User Authorization to View Packet Payload Data	114
CA Top Secret	114
CA ACF2	115
RACF	115

Chapter 11: Preparing to Start Your Product **117**

Started Task JCL Setup	117
TESTEXEC Data Set	118
Started Task Product Region Parameter Member	119
SOLVE SSI Started Task Parameter Member	120
Review and Copy the SOLVE SSI Started Task	121
Set Up OSA/SF Support	122
Review and Copy the Product Region Started Task	122
Enable the NETSTAT Interface	123
Operational Considerations	123
Subsystem Identifier Setup	123
Load Libraries	123
Authorization of the Load Libraries	124
Assign Consoles	124
Activate VTAM Applications	125
Enable Auditing by CA Auditor	125

Chapter 12: Performing Initial Migration **127**

NPF and SAF Security Members	127
------------------------------------	-----

Chapter 13: Starting Up **129**

Start the SOLVE SSI Region	129
Restart the SOLVE SSI Region	130
Start the Product Region	130
Perform the Initial Logon	131
Add the Initial Administrator User ID	131
Perform Subsequent Logon	132

Chapter 14: Customizing Your Product **135**

Initial Customization Requirements	135
Customizer Setup Types	136
Customize Parameter Values	137
Interrupted Customization	137

Update and Review the Fast Setup Customization Parameters	137
Web Browser Settings	140
Additional Parameter Groups	141
Enable Metrics Feed to CA APM	141
Implement External Applications Access	142
Implement Links to CA NetSpy Network Performance	142
Discover System Resources	142
Run Express Setup	143
Set Up the System Image to Load on Restart	144
Initialization Failures	145
Resolve Initialization Failures	145
Parameter Group Actions	146
Review Region Status	147
Perform Additional Customization	147

Chapter 15: Completing Migration 149

Knowledge Base Migration	149
Migrate Your Existing Knowledge Base	150
How to Copy Multi-Object Components	151
How to Copy Single-Object Components	151
Apply Updated Templates	152
MODS Migration	152
MODS File	153
Copy MODS Definitions	153
Panel Migration	154
Installation-Defined Panel Library	154
Individual Panels	154
Copy Panel Definitions	155
OSCNTL File Migration	156
Migrate Baseline Data	156
\$CAPKCAL \$DFDBPKG DFDBMIGRATE Procedure—Migrate Baseline Data	157
Migrate IPLOG Records	158
Region Links to a Multisystem Network	158
Important Considerations Prior to Linking	158
Link in Migration Mode	159
Migrate Subsequent Regions	159
A Multisystem Network Migration Example	160

Appendix A: Worksheets 163

Preparation Worksheets	163
Installation	163

Region Setup	168
TCP/IP Setup.....	173
Startup Tasks	175
Post-installation Worksheet	175
Appendix B: Defining UNIX System Services Authorization	177
USS Authorization Requirements	177
Set Up OMVS Segment	177
Appendix C: Tape Format	179
FMID Descriptions	179
Format of Cartridge VOLSER C2D760	180
Index	183

Chapter 1: Overview

This guide describes how to install and implement CA NetMaster NM for TCP/IP.

This section contains the following topics:

[Audience](#) (see page 11)

[How the Installation Process Works](#) (see page 11)

Audience

Readers of this book require knowledge in the following areas:

- Job control language (JCL)
- TSO/ISPF
- z/OS environment and installing software in this environment
- Your organization's IT environment, enterprise structure, and region structure

You work with the following personnel:

- Systems programmer for z/OS, VTAM, and TCP/IP definitions
- Security administrator, for library and started task access authority
- Storage Management Subsystem (SMS) or storage administrator, for direct access storage device (DASD) allocations

How the Installation Process Works

CA Technologies has standardized product installations across all mainframe products. Installation uses the following process:

- Acquisition—Transports the software to your z/OS system.
- Installation using SMP/E—Optionally creates a CSI environment and runs the RECEIVE, APPLY and ACCEPT steps. The software is untailored.
- Deployment—Copies the target libraries to another system or LPAR.
- Configuration—Creates customized load modules, bringing the software to an executable state.

CA MSM provides a web-based interface to make the standardized installation process easier. Using CA MSM, someone with limited knowledge of JCL and SMP/E can install a product.

Note: If you do not have CA MSM, you can download it from the Download Center at [the CA Support Online website](#). Follow the installation instructions in the CA Mainframe Software Manager documentation bookshelf on the CA Mainframe Software Manager product page. The standardized installation process can also be completed manually.

To install your product, do the following tasks:

1. Prepare for the installation by confirming that your site meets all installation requirements.
2. Use one of the following methods to acquire the product:
 - [Download the software from CSO using CA MSM](#) (see page 26).
 - Download the software from CSO using Pax-Enhanced Electronic Software Delivery (ESD).
 - Order a tape.
3. Perform an SMP/E installation using one of the following methods:
 - If you used CA MSM to acquire the product, start the SMP/E step from the SMP/E Environments tab in CA MSM.
 - If you used ESD to acquire the product, you can install the product in the following ways:
 - Install the product manually.
 - Use the Insert New Product option in CA MSM to complete the SMP/E installation.
 - If you used a [tape](#) (see page 71), install the product manually.

Note: If a CA Recommended Service (CA RS) package is published for your product, install it before continuing with deployment.

4. Deploy the target libraries using one of the following methods:
 - If you are using CA MSM, deployment is required; it is a prerequisite for configuration.
 - If you are using a manual process, deployment is an optional step.

Note: Deployment is considered part of starting your product.

5. Configure your product using CA MSM or manually.

Note: Configuration is considered part of starting your product.

Chapter 2: Preparing for Installation

This section contains the following topics:

[Multiple Product Installation and Setup](#) (see page 13)

[Software Requirements](#) (see page 13)

[CA Common Services Requirements](#) (see page 15)

[Security Requirements](#) (see page 16)

[Storage Requirements](#) (see page 17)

[How CA LMP Statements Are Coded](#) (see page 17)

[Worksheets](#) (see page 20)

[Migration Preparation](#) (see page 20)

Multiple Product Installation and Setup

You can install multiple products in the CA Mainframe Network Management family based on what you have purchased. You can also set up multiple products in one region.

Therefore, you can perform the steps in the *Installation Guides* for these products concurrently as you install and set them up.

Software Requirements

You must verify your system is set with the requirements described in this section.

Operating Environment

Ensure that you have the appropriate operating environment. Your system must have:

- A currently-supported version of z/OS.
- If you intend to implement Secure Sockets Layer (SSL) for the web interface:
 - SMP/E V3R5.0.
 - IBM's 31-bit SDK for z/OS, Java 2 Technology Edition for the libjvm.x side deck. IBM's 64-bit SDK is *not* supported.
- If you intend to use CA TCPaccess CS r6, ensure that you are using Service Pack 3 (SP3) or later. If SP3 is not applied, the Packet Analyzer feature does not analyze or report on the packets that flow through a CA TCPaccess CS stack.

WebCenter Requirements

WebCenter users require the following *minimum* levels of third-party products that are installed on their PCs:

- Internet Explorer: 8.0 *or* Firefox: 13.0
- Java Runtime Environment (JRE): 7

Note: If you are using a 64-bit browser, review the JRE support and minimum system requirements for 64-bit browsers on the Sun Java website.

Migration Mode

If you intend to use [migration mode](#) (see page 22) to link an Release 12.1 product region to a multisystem network at the following releases, ensure that you have applied the following APARs:

- r11.6: NY810AS (SP1)
- r11.5: RO12222 and NZ39503 (prerequisite fix NY710AS (SP1))
- r11.0: NZ39505 (prerequisite fixes NY604AS (SP2) and NZ29512)

CA Common Services Requirements

Your system must have a currently supported version of CA Common Services for z/OS. The CA Common Services load libraries must be accessible to the product address space and the SOLVE SSI address space through the JCL STEPLIB or system LNKLIST.

Note: The latest version of CA Common Services for z/OS is included in your package.

The following CA Common Services are used with CA NetMaster NM for TCP/IP:

CA LMP of the CAIRIM Common Service

Authorizes your product features. CA LMP provides a standardized and automated approach to the tracking of licensed software. The service uses common real-time enforcement software to validate the configuration. CA LMP reports on activities related to the license, usage, and financials of CA Technologies products.

CAICCI Common Service

Provides cross-system communication. This service is required, for example, for communication with Unicenter Service Desk.

CAISDI/soap

Is the z/OS Simple Object Access Protocol (SOAP) client that communicates with Unicenter Service Desk. The component manages the communication using TCP/IP to Unicenter Service Desk and provides the basic mechanisms that allow CA Technologies products to open Unicenter Service Desk tickets. This component is required for all Unicenter Service Desk integration.

Note: If other CA Technologies products are installed at your site, some of these services are already installed.

Security Requirements

When you prepare your z/OS task for startup, the following authorities are required on your system:

- If you plan to use ESD to download the product, you require access to UNIX System Services (USS).
- You have READ authority to data sets with a prefix of CAI.*.
- You have UPDATE authority to the following data sets or libraries:
 - Started task PROCLIB that stores the run-time JCL job, for example, SYS1.PROCLIB
 - SYS1.PARMLIB
 - SYS1.VTAMLST or the library that stores VTAM application definitions and VTAM initialization parameters
 - SYS1.VTAMLIB for terminal mode table definitions
 - Master catalog, a requirement if you intend to define alias entries for data set prefixes
- You have authority to update the following initialization parameter data set members if necessary:
 - SYS1.PARMLIB(IEFSSNxx) to add subsystem IDs
 - SYS1.PARMLIB(IEAAPFxx) to APF-authorize your load libraries
 - SYS1.PARMLIB(CONSOLxx) if your system does not use extended MCS consoles
 - SYS1.PARMLIB(LPALSTxx) if you want to use the SOLVE SSI task as the PPI provider
 - SYS1.PARMLIB(PROGxx) if you want CA Auditor for z/OS or CA Common Inventory Service to know of your products for your auditors
- Ensure that the following conditions are met:
 - The user IDs associated with your started tasks have access to the run-time data sets created by the installation and setup processes (UPDATE authority required).
 - The user ID associated with the product region started task is authorized to issue system commands.
 - The user IDs associated with the product and SOLVE SSI region must have authority to use [UNIX System Services](#) (see page 177).

Storage Requirements

CA NetMaster NM for TCP/IP has the following 3390 DASD space requirements:

- If you are using CA MSM or ESD, the following z/OS UNIX file system space is required for the downloaded and unpacked files: 174 MB.
- For installation and setup, the following spaces are required:
 - Installation = 1191 cylinders
 - IBM System Modification Program Extended (SMP/E) libraries = 1265 cylinders
 - Setup = 1360 cylinders
 - Setup temporary work area = 1400 cylinders

How CA LMP Statements Are Coded

Before starting this product, you must code CA LMP statements for product license authorization.

To code CA LMP statements, do the following:

1. Install CAIRIM.
2. Activate LMP.
3. Add your product license codes to the LMP statements.
4. Place the LMP statements in the KEYS member of the PPOPTION data set.

Note: The KEYS member of the PPOPTION data set is specified in the CAS9 JCL procedure. For more information, see the *CA Common Services Administration Guide*.

KEYS Member—Add Execution Key

You must add the CA LMP execution key, provided on your product key certificate, to the CAIRIM parameters to ensure proper initialization. To define a CA LMP execution key to the CAIRIM parameters, modify the KEYS member in CAI.PPOPTION (CA Common Services for z/OS r11) or CAI.CAIOPTN (CA Common Services for z/OS r12).

This sample parameter structure for KEYS member has the following format:

```
PROD(pp) DATE(ddmmyy) CPU(ddd-mmm/sssss)
LMPCODE(kkkkkkkkkkkkkkkk)
```

Parameter definitions are as follows:

PROD(pp)

Specifies the two-character product code. This code agrees with the product code already in use by the CAIRIM initialization parameters for any earlier releases of this product (if applicable).

Y7 is the value for your product.

DATE(ddmmmyy)

Specifies the CA LMP licensing agreement expiration date, for example, 13MAR12.

CPU(tttt-mmmm/ssssss)

tttt

Specifies the CPU type on which CA LMP is to run, for example, 3090.

-mmm

Specifies the CPU model on which CA LMP is to run, for example, 600.

Note: If the CPU type and or model require fewer than four characters, blank spaces are inserted for the unused characters.

/ssssss

Specifies the serial number of the CPU on which CA LMP is to run.

LMPCODE(kkkkkkkkkkkkkkk)

Specifies the execution key (kkkkkkkkkkkkkkkk) needed to run CA LMP. The key certificate shipped with each CA LMP software solution provides this CA LMP execution key.

Example: Add CA LMP Execution Key

This example shows a control statement for the CA LMP execution software parameter.

```
PROD(Y7) DATE(27JUN12) CPU(3090-600/370623)
LMPCODE(52H2K06130Z7RZD6)
```

In this example, with your product running on the specified CPU, the CA LMP licensing agreement will expire on June 27, 2012. The product code and execution key values are different when you install your product at your site.

Note: For a full description of the procedure for defining the CA LMP execution key to the CAIRIM parameters and further details about the features and associated utilities of CAIRIM, see the *CA Common Services for z/OS Administrator Guide*.

CA LMP Key Certificate

Examine the CA License Managed Program (CA LMP) key certificate. Your certificate contains the following information:

Product Name

Defines the trademarked or registered name of your product as licensed for the designated site and CPUs.

Product Code

Defines a two-character code that corresponds to the product.

Supplement

Defines the reference number of your license for a particular facility and has the following format:

nnnnnn-nnn

This format differs slightly inside and outside North America and, in some cases, the reference number may not be provided at all.

CPU ID

Defines the code that identifies the specific CPU for which installation of this product is valid.

Execution Key

Defines an encrypted code required by CA LMP for installing your product. During installation, it is referred to as the LMP code.

Expiration Date

Defines the date your license expires and has the following format:

ddmmyy

Example: 21Mar12

Technical Contact

Defines the name of the designated technical contact at your site who is responsible for the installation and maintenance of your product. CA addresses all CA LMP correspondence to this person.

MIS Director

Defines the name of the Director of MIS or the person who performs such a function at your site. If the title but not the name of the individual is indicated on the certificate, supply the actual name when correcting and verifying the certificate.

CPU Location

Defines the address of the building in which the CPU is installed.

Worksheets

The [preparation worksheets](#) (see page 163) help you gather the required information before you install and configure (or set up) the product.

The [post-installation worksheet](#) (see page 175) lets you record the names of the data sets created by the installation and configuration process for future reference.

Migration Preparation

Some migration tasks require actions on the region that you are migrating from. If you are planning to reuse resources for your new product region, such as access control block (ACB) name and started task name, make sure that you perform these tasks before you shut down your existing region for the last time.

More information:

[Performing Initial Migration](#) (see page 127)

[Completing Migration](#) (see page 149)

Parameter Group Values

If you do not use a region initialization (INI) file and want to migrate your previous parameter group values to your new product region, record these values now. You use them to customize the product region.

How to Migrate Your Initialization File

If you have an existing region INI file from r11 onwards, you can migrate the file for use in this release.

Important! Review and update the file to ensure that names such as ACBs, data sets, and interfaces are suitable for the new region.

The process of migrating your INI file consists of the following steps:

1. If you have not already generated your INI file, generate the INI file in the previous region.
2. Configure the file by updating the data set names used, and checking the ACB and various interface names. Alternatively, you can delete the configuration section for a whole parameter group to let the defaults for the new region be used.

Note: During region initialization, the INI file is applied by passing all parameter values to the INI file procedure and letting the procedure overwrite the values as needed. If you do not want to overwrite the settings for a parameter group or individual parameter, comment out or delete the statements in the INI file that contains the group or parameter. Setting the value of a parameter to null sets the parameter value to null, which may not be what you wanted.

3. Start the new region using the INI file by editing your RUNSYSIN.

After you start the region, you can check it and regenerate the INI if necessary.

Important! Generation of the INI file replaces custom code, such as code that includes MVS system symbols, with the actual values. If you regenerate the file, reapply the custom code.

Note: For more information about setting up the initialization file, see the *Administration Guide*.

Knowledge Base

If you want to migrate your knowledge base, and you want to keep a copy of an old distributed template (for example, you might have modified it), copy this template to a new template image version above 0009.

Multisystem Considerations

You cannot link and synchronize a new region with a region running an earlier release of the product.

How Migration Mode Works

You can use migration mode to assist in the migration of an existing multisystem network.

Migration mode gives the new product region the same level of visibility as normal synchronization, but a slightly reduced command capability. The main difference between migration mode and normal synchronization is that the databases are not synchronized, and single point database maintenance is not possible in migration mode.

Migration mode works as follows:

1. You unlink an existing region from the multisystem network.
2. You migrate this region to the latest release.
3. You link the newly-migrated region back into the multisystem network.
4. After the new region is linked back, you can monitor all resources for all linked regions from the new region.
5. When the next region is unlinked and migrated to the latest release, it can be linked and synchronized in the standard way to the first migrated region.

Each region can be migrated as required without losing the benefits of multisystem monitoring.

More information:

[Software Requirements](#) (see page 13)

How to Prepare for Multisystem Network Migration

If you are upgrading multiple synchronized regions to this release, perform the following steps to plan for it.

1. Ensure that your existing multisystem network has at least two focal regions. If you have only one focal region, unlink a subordinate region and relink it as a focal region.
2. Choose a focal region and unlink it from the multisystem network.
3. Upgrade the focal region, and perform migration tasks.
4. After you have completed all of the steps in this guide, [link your new focal region in migration mode](#) (see page 158) to an existing focal region.
5. Select the next product region to upgrade and unlink it.
6. Upgrade this product region and then synchronize it to the focal region that you upgraded in Step 3.
7. Continue until all regions are upgraded.

Notes:

- You only perform knowledge base migration for the first region because the focal knowledge base contains details of all linked regions.
- You only link the first new focal region in migration mode.

Chapter 3: Installing Your Product Using CA MSM

Use the procedures in this section to manage your product using CA MSM. Managing includes acquiring, installing, maintaining, and deploying products, setting system registries, and managing your CSIs. These procedures assume that you have already installed and configured CA MSM.

Note: If you do not have CA MSM, you can download it from the Download Center at [the CA Support Online website](#). Follow the installation instructions in the CA Mainframe Software Manager documentation bookshelf on the CA Mainframe Software Manager product page.

When you have completed the procedures in this section, go to Configuring Your Product.

This section contains the following topics:

[How to Use CA MSM: Scenarios](#) (see page 26)

[Access CA MSM Using the Web-Based Interface](#) (see page 34)

Important! During installation, use the CAIT76 target zone and the CAID76 distribution zone. The setup process requires that these zone names be used.

These topics provide information to get you started managing your product using CA MSM. You can use the online help included in CA MSM to get additional information.

Before using these topics, you must already have CA MSM installed at your site. If you do not have CA MSM installed, you can download it from the Download Center at [the CA Support Online website](#), which also contains links to the complete documentation for CA MSM.

How to Use CA MSM: Scenarios

Imagine that your organization has started using CA MSM to simplify the installation of CA Technologies products and unify their management. You have also licensed a new CA Technologies product. In addition, you have a number of existing SMP/E environments from previously installed CA Technologies products.

You can use the following scenarios to guide you through the process:

1. [Acquire the new product](#) (see page 26).
2. [Install the new product](#) (see page 27).
3. [Maintain products already installed in your environment](#) (see page 29).
4. [Set up the CA MSM system registry](#) (see page 30).
5. [Deploy the product to your target systems](#) (see page 32).
6. [Configure the deployed product to your target systems](#) (see page 33).

How to Acquire a Product

The *Product Acquisition Service (PAS)* facilitates the acquisition of mainframe products and the service for those products, such as program temporary fixes (PTFs). The PAS retrieves information about products to which your site is entitled. Then it records these entitlements in a software inventory that is maintained on your driving system.

You can use the PAS component of CA MSM to acquire a CA Technologies product.

You perform the following high-level tasks to acquire a product using CA MSM:

1. Set up a CA Support Online account.

To use CA MSM to acquire or download a product, you must have a CA Support Online account. If you do not have an account, you can create one on [the CA Support Online website](#).
2. Determine the CA MSM URL for your site.

To [access CA MSM](#) (see page 34), you require its URL. You can get the URL from your site CA MSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA MSM account with your credentials for [the CA Support Online website](#). This account enables you to download product packages.

3. Log in to CA MSM and go to the Software Catalog page to locate the product that you want to manage.

After you log in to CA MSM, you can see the products to which your organization is entitled on the Software Catalog tab.

If you cannot find the product that you want to acquire, update the catalog. CA MSM refreshes the catalog through [the CA Support Online website](#) using the site IDs associated with your credentials for [the CA Support Online website](#).

4. Download the product installation packages.

After you find your product in the catalog, you can download the product installation packages.

CA MSM downloads (acquires) the packages (including any maintenance packages) from the CA FTP site.

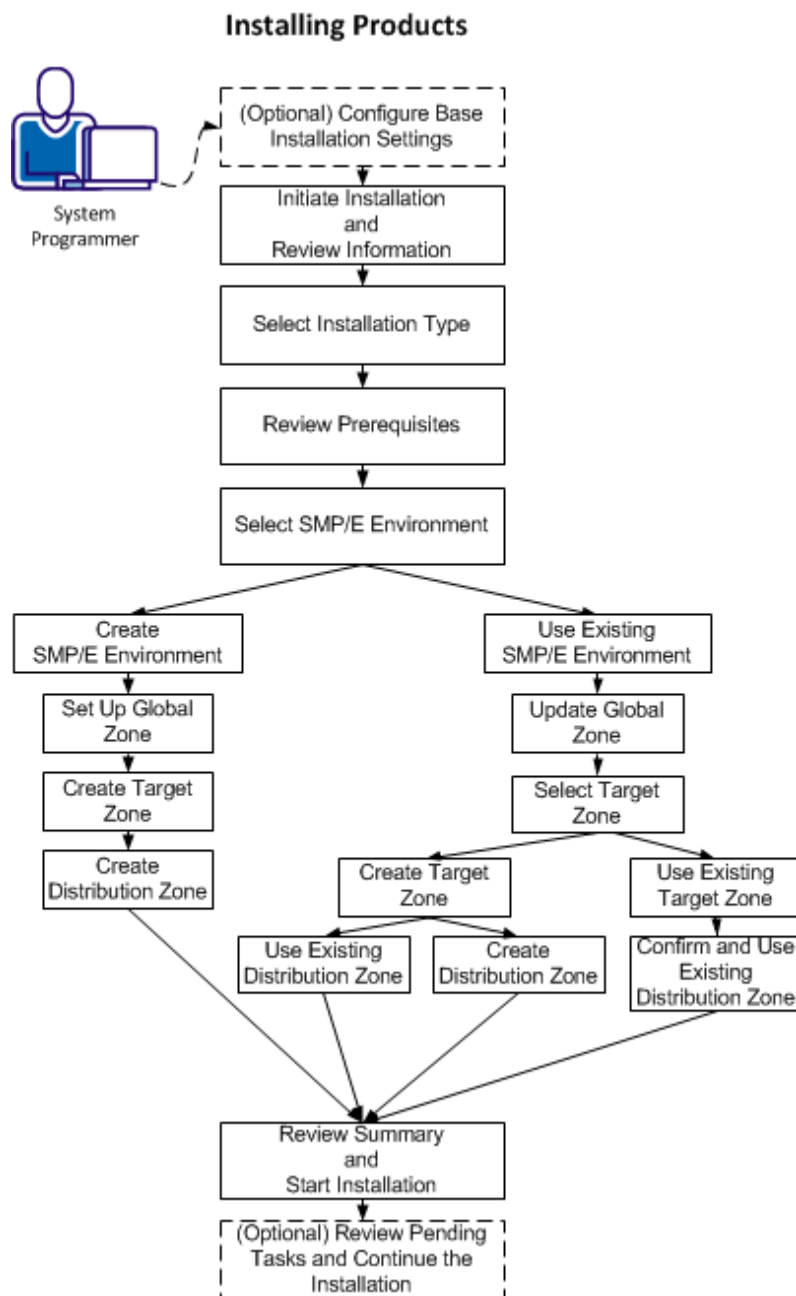
After the acquisition process completes, the product is ready for you to install or maintain.

How to Install a Product

The *Software Installation Service (SIS)* facilitates the installation and maintenance of mainframe products in the software inventory of the driving system. This facilitation includes browsing downloaded software packages, managing SMP/E consolidated software inventories on the driving system, and automating installation tasks.

You can use the SIS component of CA MSM to install a CA Technologies product.

You perform the following high-level tasks to install a product using CA MSM:



1. (Optional) Configure base installation settings.
2. Initiate product installation and review product information.
3. Select an installation type.
4. Review installation prerequisites if any are presented.

5. Take *one* of the following steps to select an SMP/E environment:
 - Create an SMP/E environment:
 - a. Set up the global zone.
 - b. Create a target zone.
 - c. Create a distribution zone.
 - Use an existing SMP/E environment from your working set:
 - a. Update the global zone.
 - b. Set up the target zone: Either create a target zone or use an existing target zone.
 - c. Set up the distribution zone: Either create a distribution zone or use an existing distribution zone.
- Note:** If you install a product or its components into an existing target or distribution zone, older versions are deleted from the zone and associated data sets. We recommend that you use new target and distribution zones for this installation so that you can apply maintenance to your current version, if necessary.
6. Review the installation summary and start the installation.
7. (Optional) Review pending tasks for the SMP/E environment where you are installing your product. Continue the installation, if applicable.

After the installation process completes, check for and install available product maintenance. The product is ready for you to deploy. Sometimes there are other steps to perform manually outside of CA MSM before beginning the deployment process.

More information:

[How to Maintain Existing Products](#) (see page 29)

How to Maintain Existing Products

You can migrate existing SMP/E environments into CA MSM to maintain all your installed products in a unified way from a single web-based interface.

You can use CA MSM to maintain a CA Technologies product.

You perform the following high-level tasks to maintain a product using CA MSM:

1. Migrate the SMP/E environment to CA MSM to maintain an existing SMP/E environment in CA MSM.

During the migration, CA MSM stores information about the SMP/E environment in the database.

2. Download the latest maintenance for the installed product releases from the Software Catalog tab.

If you cannot find the required release, you can perform the following steps to download the maintenance:

- a. Add the release to the catalog manually.
 - b. Update the release.
3. Apply the maintenance.

Note: You can also install maintenance to a particular SMP/E environment from the SMP/E Environments tab.

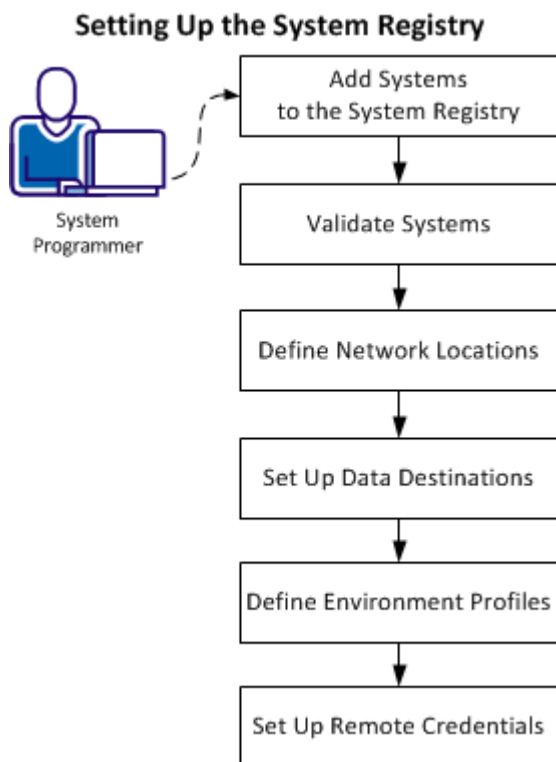
After the maintenance process completes, the product is ready for you to deploy. Sometimes there are other steps to perform manually outside of CA MSM before beginning the deployment process.

How to Set Up the System Registry

The *system registry* is a repository of variable data that all CA MSM managed products share. The system registry repository contains information about the systems that have been defined to CA MSM and selected as a target for deployments and configurations. You can create non-sysplex, sysplex, shared DASD cluster, and staging systems. You can maintain, validate, view, and delete a registered system and you can investigate a failed validation.

For each system that you register, there is one entry. Each entry consists of three categories of information: general, network locations, and data destinations.

You perform the following tasks to set up the system registry in CA MSM:



1. Add systems to the system registry.
2. Validate systems.
3. Define network locations.
4. Set up data destinations.
5. Define environment profiles.
6. Set up remote credentials.

Add and then validate each nonstaging system in the enterprise that you are deploying to, to the CA MSM system registry. You can only send a deployment to a validated system.

This process applies to each nonstaging system in your enterprise. For example, if you have five systems at your enterprise, then perform this process five times.

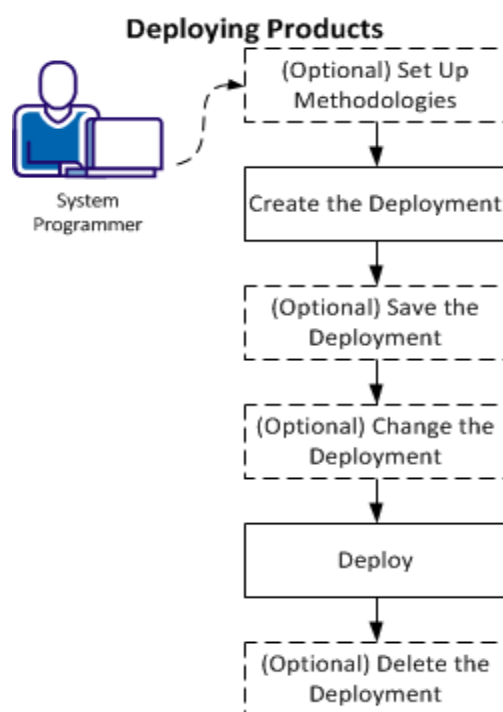
Note: After a system is validated, there is no need to validate it again. However, you can revalidate a system any time.

How to Deploy a Product

The *Software Deployment Service (SDS)* facilitates the mainframe product deployment from the software inventory of the driving system to the target system. This facilitation includes deploying installed products that are policy-driven with a set of appropriate transport mechanisms across a known topology.

You can use the SDS component of CA MSM to deploy a CA Technologies product that you have already acquired and installed.

You perform the following high-level tasks to deploy your products using CA MSM:



1. (Optional) Set up methodologies.
Note: You can also set up methodologies when creating a deployment.
2. Create the deployment.
3. (Optional) Save the deployment for editing and deploying later.
4. (Optional) Change the deployment: Add and edit systems, products, custom data sets, and methodologies.

5. Deploy:
 - a. Take a snapshot.
 - b. Transmit to target.
 - c. Deploy (unpack) to mainframe environment.
6. (Optional) Delete the deployment.

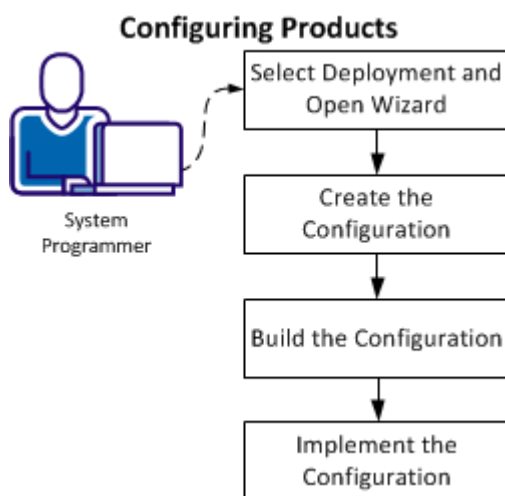
After the deployment process completes, the product is ready for you to configure. Sometimes there are other steps to perform manually outside of CA MSM before beginning the configuration process.

How to Configure a Product

The *Software Configuration Service (SCS)* facilitates the mainframe product configuration from the software inventory of the driving system to targeted z/OS operating systems.

You can use the SCS component of CA MSM to configure a CA Technologies product that you have already acquired, installed, and deployed.

You perform the following high-level tasks to configure your products using CA MSM:



1. From the Deployments tab, select a configurable deployment, select the associated product, and click Create Configuration to open the Configuration wizard.
2. Create the configuration by completing all the steps in the wizard:
 - a. Define a configuration name and select a target system.
 - b. Select configuration functions and options.
 - c. Define system preferences.
 - d. Create target settings.
 - e. Select and edit resources.
3. Build the configuration. The last step of the Configuration wizard lets you build the configuration. If needed, you can edit the configuration and can build the configuration again.
4. Implement the configuration. The implementation process in CA MSM guides you and provides detailed instructions to start, stop, and manage the steps of the implementation process.

After the configuration process completes, the product is ready for you to use. Sometimes there are other steps to perform manually outside of CA MSM.

Note: You cannot use CA MSM to configure a product to a staging system.

Access CA MSM Using the Web-Based Interface

You access CA MSM using the web-based interface.

You need the URL of CA MSM from the CA MSM administrator.

Follow these steps:

1. Start your web browser, and enter the access URL.

The login page appears.

Note: If the Notice and Consent Banner appears, read and confirm the provided information.

2. Enter your z/OS login user name and password.

The initial page appears. If you log in for the first time, you are prompted to define your account on [the CA Support Online website](#).

Note: For more information about the interface, click the online help link at the top right corner of the page.

3. Click New.

You are prompted for the credentials to use on [the CA Support Online website](#).

4. Specify the credentials, click OK, and then click Next.

You are prompted to review your user settings.

Note: These settings are available on the User Settings page.

5. Change the settings or keep the defaults, and then click Finish.

A dialog opens, which shows the progress of the configuration task. You can click Show Results to view the details of the actions in a finished task.

Important! If your site uses proxies, review your proxy credentials on the User Settings, Software Acquisition page.

Chapter 4: Installing Your Product from Pax-Enhanced ESD

This section contains the following topics:

[How to Install a Product Using Pax-Enhanced ESD](#) (see page 37)

[Allocate and Mount a File System](#) (see page 43)

[Copy the Product Pax Files into Your USS Directory](#) (see page 46)

[Create a Product Directory from the Pax File](#) (see page 51)

[Copy Installation Files to z/OS Data Sets](#) (see page 52)

[Unload the Install Utility](#) (see page 53)

[Installation JCL](#) (see page 54)

[Clean Up the USS Directory](#) (see page 57)

[Maintenance](#) (see page 58)

How to Install a Product Using Pax-Enhanced ESD

This section describes the Pax-Enhanced ESD process. We recommend that you read this overview and follow the entire procedure the first time you complete a Pax-Enhanced ESD installation. For experienced UNIX users, the *Pax-Enhanced ESD Quick Reference Guide* has sufficient information for subsequent installations.

Important! Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories used for the ESD process.

If you prefer not to involve all CA Technologies product installers with z/OS UNIX System Services, assign a group familiar with USS to perform Steps 1 through 4 and provide the list of the unpacked MVS data sets to the product installer. USS is not required for the actual SMP/E RECEIVE of the product or for any of the remaining installation steps.

To install files using Pax-Enhanced ESD, use the following process:

1. Allocate and mount the file system. This process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system dedicated to Pax-Enhanced ESD and create the directory in this file system. Ensure that all users who will be working with pax files have write authority to the directory.

2. Copy the product pax files into your USS directory. To download files, choose one of the following options:

- Download a zip file from CA Support Online to your PC, unzip the file, and then upload the product pax files to your USS file system.
- FTP the pax files from CA Support Online directly to your USS directory.

Note: Perform Steps 3 through 6 for each pax file that you upload to your USS directory.

3. Create a product directory from the pax file. Set the current working directory to the directory containing the pax file, and create a new directory in your USS directory by entering the following command:

```
pax -rvf pax-filename
```

4. Use the SMP/E GIMUNZIP utility to create z/OS installation data sets. The file UNZIPJCL in the directory created by the pax command in Step 3 contains a sample job to GIMUNZIP the installation package. Edit and submit the UNZIPJCL job.
5. Proceed with product installation. Consult product-specific documentation, including AREADME files and installation notes to complete the product installation.
6. (Optional) Clean up the USS directory. Delete the pax file, the directory created by the pax command, all of the files in it, and the SMP/E RELFILES, SMPMCS, and HOLDDATA data sets.

More Information:

[USS Environment Setup](#) (see page 42)

[Allocate and Mount a File System](#) (see page 43)

[Copy the Product Pax Files into Your USS Directory](#) (see page 46)

[Create a Product Directory from the Pax File](#) (see page 51)

[Copy Installation Files to z/OS Data Sets](#) (see page 52)

How the Pax-Enhanced ESD Download Works

Important! To download pax files for the SMP/E installation as part of the Pax-Enhanced ESD process, you must have write authority to the UNIX System Services (USS) directories used for the ESD process and available USS file space before you start the procedures in this guide.

Use the following process to download files using Pax-Enhanced ESD:

1. Log in to <https://support.ca.com/>, and click Download Center.

The CA Support Online web page appears.

2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and genlevel (if applicable), and click Go.

The CA Product Download window appears.

3. Download an entire CA Technologies product software package or individual pax files to your PC or mainframe. If you download a zip file, you must unzip it before continuing.

For both options, [The ESD Product Download Window](#) (see page 39) topic explains how the download interface works.

Note: For traditional installation downloads, see the *Traditional ESD User Guide*. Go to <https://support.ca.com/>, log in, and click Download Center. A link to the guide appears under the Download Help heading.

4. Perform the steps to install the product based on the product-specific steps.

The product is installed on the mainframe.

ESD Product Download Window

You can download CA Technologies product ESD packages multiple ways. Your choices depend on the size of the individual files and the number of files that you want to download. You can download the complete product with all components, or you can select individual pax and documentation files for your product or component.

The following illustration shows sample product files. The illustration lists all components of the product. You can use the Download Cart by selecting one or more components that you need, or selecting the check box for Add All to cart. If you prefer to immediately download a component, click the Download link.

CA Earl - MVS

- [Pax Enhanced Electronic Software Delivery \(ESD\) Guide](#)
- [Pax Enhanced Electronic Software Delivery \(ESD\) Quick Reference Guide](#)
- [Traditional Electronic Software Delivery \(ESD\) Guide](#)
- [Learn more about Using pkzip with your Downloaded Mainframe Products](#)
- [Learn more about downloading components of CA product](#)
- [Mounting ISO Images with OpenVMS](#)

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

Note: Related Published Solutions are available on the other results tab on this page. You must add these solutions to your Download Cart to include them with your product files for download.

[View Download Cart](#)

				☐ Add All to cart	
Product Components				Add to cart	Download
CCS - LEGACY - ESD ONLY 140000AW030.pax.Z	14.0 /0000	07/06/2011	4.89MB	☐	Download
CCS - MFNSM - ESD ONLY 140000AW040.pax.Z	14.0 /0000	07/06/2011	202.01MB	☐	Download
CCS - BASE - ESD ONLY 140001AW010.pax.Z	14.1 /0000	06/05/2012	27.44MB	☐	Download
CCS - OPTIONAL - ESD ONLY 140001AW020.pax.Z	14.1 /0000	06/05/2012	14.49MB	☐	Download
CA EARL PRODUCT PACKAGE 610106AEO00.pax.Z	6.1 /0106	10/30/2008	1.85MB	☐	Download
EARL PIPPACK AEO61010600.pdf	6.1 /0106	01/29/2010	93.92KB	☐	Download
CA EASYTRIEVE PRODUCT PACKAGE B60000ESA00.pax.Z	11.6 /0000	07/05/2011	6.12MB	☐	Download
DATACOM/AD PROD INFO PACKET CAIE00000P0.pdf	14.0 /0000	06/01/2012	220.53KB	☐	Download
DATACOM/AD XPRESS INSTALL				☐	Download

Clicking the link for an individual component takes you to the Download Method page.

Download Method

Please choose a download method to complete your download request. [Learn More](#)

HTTP via Download Manager

This is the CA recommended method for download. The Download Manager allows you to download your files faster and more efficiently.

[Download](#)

HTTP via Internet Browser

If Download Manager cannot be used or fails to start you may access your file(s) via your internet browser.

[View File Link\(s\)](#)

FTP

This method allows you to download your file(s) via FTP from CA's content delivery network or via native FTP servers.

Note: Processing is required and an email notification will be sent when your request is ready for downloading.

[FTP Request](#)

Depending on the size and quantity of ordered product files, the Download Method screen could also have these options:

Note: For mainframe downloads using this HTTP method, click the Learn More link.

Download Method

Please choose a download method to complete your download request. [Learn More](#)

HTTP via Download Manager

This is the CA recommended method for download. The Download Manager allows you to download your files faster and more efficiently.

[Download](#)

Create a Zip File

This method allows you to bundle your download files into one or more zip files of up to 3.5 GB each. These zip files can then be downloaded via HTTP or FTP.

Note: Processing is required and an email notification will be sent when your request is ready for downloading.

[Create Zip](#)

The HTTP method lets you start downloading immediately. The FTP method takes you to the Review Orders page that displays your order, first in a Pending status changing to Ready when your order has been processed.

Preferred FTP uses the new content delivery network (CDN). Alternate FTP uses the CA Technologies New York-based FTP servers.

The Create a Zip File option first creates the zip, and when ready, offers the options that the Zip Download Request examples show in the next illustration.

Review Download Requests

Below is a list of the FTP and large HTTP downloads that have been requested by your site. When status is set to **'Ready'** a link will appear.

- For FTP requests, click on the FTP link to view the path information for your download. For more information view our [FTP Help document](#)
- For HTTP requests, click on the HTTP link to initiate your download.
- To view the details of your request, click on the desired order number.

Today's Downloads

Order #	Status	Description	Date Placed	Download Options
10000961	Ready	FTP Download Request	04/30/2010	Preferred FTP ▾ Alternate FTP ▾

Previous 6 day Download History

Order #	Status	Description	Date Placed	Download Options
10000949	Ready	ZIP Download Request	04/29/2010	HTTP via DLM Preferred FTP ▾ Alternate FTP ▾
10000948	Ready	ZIP Download Request	04/29/2010	HTTP via DLM Preferred FTP ▾ Alternate FTP ▾

USS Environment Setup

You need a UNIX System Services (USS) directory and a file system with adequate space to perform the following tasks:

- Receive product pax files from CA Support Online.
- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.

We recommend that you allocate and mount a file system dedicated to Pax-Enhanced ESD. The amount of space that you need for the file system depends on the following variables:

- The size of the pax files that you intend to download.
- Whether you plan to keep the pax files after unpacking them. We do not recommend this practice.

We recommend that you use one directory for downloading and unpacking pax files. Reusing the same directory minimizes USS setup. You need to complete the USS setup only one time. You reuse the same directory for subsequent downloads. Alternatively, you can create a new directory for each pax download.

Important! Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories used for the ESD process. In the file system that contains the ESD directories, you also need free space approximately 3.5 times the pax file size to download the pax file and unpack its contents. For example, to download and unpack a 14 MB pax file, you need approximately 49 MB of free space in the file system hosting your ESD directory.

Allocate and Mount a File System

You can use the zSeries File System (zFS) or hierarchical file system (HFS) for ESD downloads.

This procedure describes how to perform the following tasks:

- Allocate a zFS or an HFS.
- Create a mount point in an existing maintenance USS directory of your choice.
- Mount the file system on the newly created mount point.

Note: You must have SUPERUSER authority to do this.

- Optionally, permit write access to anyone in the same group as the person who created the directory.

Important! USS commands are case-sensitive.

Follow these steps:

1. Allocate the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
//DEFINE EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//AMSDUMP DD SYSOUT=*
//SYSIN DD *
  DEFINE CLUSTER ( +
    NAME(your_zFS_data_set_name) +
    STORAGECLASS(class) +
    LINEAR +
    CYL(primary secondary) +
    SHAREOPTIONS(3,3) +
  )
/*
//FORMAT EXEC PGM=IOEAGFMT,REGION=0M,
// PARM=(' -aggregate your_zFS_data_set_name -compat' )
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
//CEEDUMP DD SYSOUT=*
/*
```

- On an HFS, use the following sample:

```
//ALCHFS EXEC PGM=IEFBR14
//CAESD DD DSN=yourHFS_data_set_name,
// DISP=(NEW,CATLG,DELETE),UNIT=3390,
// DSN TYPE=HFS,SPACE=(CYL,(primary,secondary),1)
```

The file system is allocated.

Note: Ensure that the zFS or HFS data set name that you use conforms to your data set naming conventions for USS file systems. If the allocation of the file system data set fails, it is because of environmental settings not allowing for the allocation. On an HFS, try using the ISPF 3.2 Data Set Utility to allocate your HFS data set.

2. Create a mount point for the file system. This example shows how to create a /CA/CAESD directory in an existing directory, /u/maint. From the TSO OMVS shell, enter the following commands:

```
cd /u/maint/  
mkdir CA  
cd CA  
mkdir CAESD
```

Note: This document refers to this structure as *yourUSSESDdirectory*.

The mount point is created.

3. Mount the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
MOUNT FILESYSTEM('your_zFS_data_set_name')  
      MOUNTPOINT('yourUSSESDdirectory')  
      TYPE(ZFS)  MODE(RDWR)  
      PARM(AGGROW)
```

- On an HFS, use the following sample:

```
MOUNT FILESYSTEM('your_HFS_data_set_name')  
      MOUNTPOINT('yourUSSESDdirectory')  
      TYPE(HFS)  MODE(RDWR)
```

The file system is mounted.

4. (Optional) Set security permissions for the directory. You can use the chmod command to let other users access the ESD directory and its files. For example, to allow write access to the ESD directory for other users in your USS group, from the TSO OMVS shell, enter the following command:

```
chmod -R 775 /yourUSSESDdirectory/
```

Write access is granted.

Note: For more information about the chmod command, see the IBM *z/OS UNIX System Services User Guide* (SA22-7802).

Copy the Product Pax Files into Your USS Directory

To begin the CA Technologies product installation procedure, copy the product pax file into the USS directory that you set up. Use one of the following methods:

- Download the product pax files directly from the CA Support Online FTP server to your z/OS system.
- Download the product pax file from the CA Support Online FTP server to your computer, and upload it to your z/OS system.
- Download the product file from CA Support Online to your computer. If your download included a zip file, unzip the file, and upload the unzipped pax files to your z/OS system.

This section includes a sample batch job to download a product pax file from the CA Support Online FTP server directly to a USS directory on your z/OS system and sample commands to upload a pax file from your computer to a USS directory on your z/OS system.

Important! The FTP procedures vary due to local firewall and other security settings. Consult your local network administrators to determine the appropriate FTP procedure to use at your site.

Ensure that sufficient free space is available in the USS file system that you are using for Pax-Enhanced ESD to hold the product pax file. If you do not have sufficient free space, error messages similar to the following appear:

```
EZA1490I Error writing to data set  
EZA2606W File I/O error 133
```

When the download finishes, the pax file size in your USS directory matches the value in the Size column for the corresponding pax file on the CA Technologies Products Download window.

More Information:

[How the Pax-Enhanced ESD Download Works](#) (see page 39)
[ESD Product Download Window](#) (see page 39)

Download Using Batch JCL

Use this process to download a pax file from the CA Support Product Downloads window by running batch JCL on the mainframe. Use the sample JCL attached to the PDF file as CAtoMainframe.txt to perform the download.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the file to view the sample JCL.

Note: We recommend that you follow the preferred method as described on CA Support Online. This procedure is our preferred download method; however, we do include the procedure to download to the mainframe through a PC in the next section.

Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.
The job points to your profile.
3. Replace *YourEmailAddress* with your email address.
The job points to your email address.
4. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.
The job points to your USS directory.
5. Locate the product component to download on the CA Support Product Download window.
You have identified the product component to download.
6. Click Download for the applicable file.
Note: For multiple downloads, add files to a cart.
The Download Method window opens.
7. Click FTP Request.
The Review Download Requests window displays any files that you have requested to download.

Note: We send you an email when the file is ready to download or a link appears in this window when the file is available.

8. Select one of the following methods:

Preferred FTP

Uses CA Technologies worldwide content delivery network (CDN). If you cannot download using this method, review the security restrictions for servers that company employees can download from that are outside your corporate network.

Host Name: ftp://ftpdnloads.ca.com

Alternate FTP

Uses the original download servers that are based on Long Island, New York.

Host Name: ftp://scftpd.ca.com for product files and download cart files and ftp://ftp.ca.com for individual solution files.

Both methods display the host, user name, password, and FTP location, which you then can copy into the sample JCL.

Note: The following links provide details regarding FTP: the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

Important! If your FTP commands are incorrect, it is possible for this job to fail and still return a zero condition code. Read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

After you run the JCL job, the pax file resides in the mainframe USS directory that you supplied.

Example: CAtoMainframe.txt, JCL

The following text appears in the attached CAtoMainframe.txt JCL file:

```
//GETPAX JOB (ACCOUNTNO),'FTP GET ESD PACKAGE',
//          MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to download a pax file directly from *
/* CA Support Online to a USS directory on your z/OS system.      *
/*                                                                *
/* When editing the JCL ensure that you do not have sequence numbers *
/* turned on.                                                    *
/*                                                                *
/* This job must be customized as follows:                        *
/* 1. Supply a valid JOB statement.                               *
/* 2. The SYSTCPD and SYSFTPD JCL DD's statements in this JCL maybe *
/*    optional at your site. Remove the statements that are not  *
/*    required. For the required statements, update the data set  *
/*    names with the correct site specific data set names.       *
/* 3. Replace "Host" based on the type of download method.       *
/* 4. Replace "YourEmailAddress" with your email address.        *
/* 5. Replace "yourUSSESDdirectory" with the name of the USS     *
/*    directory used on your system for ESD downloads.           *
/* 6. Replace "FTP Location" with the complete path              *
/*    and name of the pax file obtained from the FTP location   *
/*    of the product download page.                              *
//*****
//GETPAX EXEC PGM=FTP,PARM='(EXIT',REGION=0M
//SYSTCPD DD DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSFTPD DD DSN=yourFTP.DATA.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//OUTPUT DD SYSOUT=*
//INPUT DD *
Host
anonymous YourEmailAddress
lcd yourUSSESDdirectory
binary
get FTP location
quit
```

Download Files to Mainframe through a PC

If you download pax or zip files from CA Support Online to your PC, use this procedure to upload the pax file from your PC to your z/OS USS directory.

Follow these steps:

1. Follow the procedures in How the Pax-Enhanced ESD Download Works to download the product pax or zip file to your PC. If you download a zip file, first unzip the file to use the product pax files.

The pax or zip file resides on your PC.

2. Open a Windows command prompt.

The command prompt appears.

3. Customize and enter the FTP commands with the following changes:
 - a. Replace *mainframe* with the z/OS system's IP address or DNS name.
 - b. Replace *userid* with your z/OS user ID.
 - c. Replace *password* with your z/OS password.
 - d. Replace *C:\PC\folder\for\thePAXfile* with the location of the pax file on your PC.
 - e. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.
 - f. Replace *paxfile.pax.Z* with the name of the pax file to upload.

The pax file is transferred to the mainframe.

Example: FTP Commands

This list is a sample of FTP commands to upload the pax file from your PC to your USS Pax-Enhanced ESD directory:

```
ftp mainframe
userid
password
bin
lcd C:\PC\folder\for\thePAXfile
cd /yourUSSESDdirectory/
put paxfile.pax.Z
quit
exit
```

Create a Product Directory from the Pax File

Use the sample job attached to the PDF file as Unpackage.txt to extract the product pax file into a product installation directory.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the file to view the sample JCL.

Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

The job points to your specific directory.

3. Replace *paxfile.pax.Z* with the name of the pax file.

The job points to your specific pax file.

4. Submit the job.

The job runs and creates the product directory.

Note: If the PARM= statement exceeds 71 characters, uncomment and use the second form of UNPAXDIR instead. This sample job uses an X in column 72 to continue the PARM= parameters to a second line.

Sample Job to Execute the Pax Command (Unpackage.txt)

The following text appears in the attached Unpackage.txt JCL file:

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX ESD PACKAGE ',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to invoke the pax command to create *
/* the product-specific installation directory. *
/* *
/* This job must be customized as follows: *
/* 1. Supply a valid JOB statement. *
/* 2. Replace "yourUSSESDdirectory" with the name of the USS *
/* directory used on your system for ESD downloads. *
/* 3. Replace "paxfile.pax.Z" with the name of the pax file. *
/* NOTE: If you continue the PARM= statement on a second line, make *
/* sure the 'X' continuation character is in column 72. *
//*****
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSESDdirectory/; pax -rvf paxfile.pax.Z'
/*UNPAXDIR EXEC PGM=BPXBATCH,
/* PARM='sh cd /yourUSSESDdirectory/; pax X
/* -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

Copy Installation Files to z/OS Data Sets

Use this procedure to invoke the SMP/E GIMUNZIP utility to create MVS data sets from the files in the product-specific directory.

Follow these steps:

1. Locate and read the product readme file or installation notes, if applicable, which resides in the product-specific directory that the pax command created. This file contains the product-specific details you require to complete the installation procedure.

You have identified the product-specific installation details.

2. Use ISPF EDIT or TSO ISHELL to edit the UNZIPJCL sample job. You can perform this step in one of the following ways:
 - Use ISPF EDIT. Specify the full path name of the UNZIPJCL file.
 - Use TSO ISHELL. Navigate to the UNZIPJCL file and use the E line command to edit the file.

The job is edited.

3. Change the SMPDIR DD PATH to the product-specific directory created by the pax command.

Your view is of the product-specific directory.

4. If ICSF is not active, perform the following steps:
 - a. Change the SMPJHOME DD PATH to your Java runtime directory. This directory varies from system to system.
 - b. Perform one of the following steps:
 - Change the SMPCPATH DD PATH to your SMP/E Java application classes directory, typically /usr/lpp/smp/classes/.
 - Change HASH=YES to HASH=NO on the GIMUNZIP parameter.

One of the following occurs: ICSF is active or you are using Java.

5. Change all occurrences of *yourHLQ* to the high-level qualifier (HLQ) for z/OS data sets used by the installation process. We suggest that you use a unique HLQ for each expanded pax file to identify uniquely the package. Do *not* use the same value for *yourHLQ* as you use for the SMP/E RELFILES.

All occurrences of *yourHLQ* are set to your high-level qualifier for z/OS data sets.

6. Submit the UNZIPJCL job.

The UNZIPJCL job completes with a zero return code. Messages GIM69158I and GIM48101I in the output and IKJ56228I in the JES log are acceptable.

GIMUNZIP creates z/OS data sets with the high-level qualifier you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed.

Note: For more information, see the IBM reference guide, *SMP/E for z/OS Reference (SA22-7772)*.

Unload the Install Utility

The installation utility software lets you generate and run the JCL required to install your product. The installation utility software is delivered electronically with ESD.

The installation software unloads into the *dsnpref.CAI.NMC1.CC2DJCL* data set; *dsnpref* is a prefix you specify for your product data sets.

After you unzip the data sets, do *one* of the following:

- Rename *dsnpref.CAI.NMC1.CC2DJCL* to *dsnpref.NMC1.CC2DJCL*
- Copy the members in *dsnpref.CAI.NMC1.CC2DJCL* into *dsnpref.NMC1.CC2DJCL*

Additional Features

The Install Utility provides an option to install the following additional features:

- SSL support
- ReportCenter

Install, set up, and customize your product region completely before installing ReportCenter.

Note: For information about installing these features, see the *ReportCenter Guide*.

Installation JCL

The installation process creates the *dsnpref.NMC1.INSTDB* database to store details of each installation that you perform. If you are also installing other products in the CA Mainframe Network Management family of products, this database manages those installations. These details include the products you install and the installation values that you specify.

Note: During this task, the INSTALLATION JCL Library Creation panel lets you specify your installation JCL library. The default library name is *dsnpref.NMC1.INSTALL.JCL*, where *dsnpref* is the same data set prefix you used for the *dsnpref.NMC1.CC2DJCL* data set.

If your installation JCL library exists, do *one* of the following:

- Specify a new data set name at that panel.
- Delete the existing library by issuing a TSO DELETE command.

Note: If you leave the Install Utility at any stage, you can return to it from the ISPF/PDF TSO Command Shell prompt. Execute the following command:

```
EXEC 'dsnpref.NMC1.CC2DJCL(INSTALL)'
```

Generate the Installation JCL

During the installation process, you provide the [site-specific installation information that you previously collected](#) (see page 163). This information is used to generate the installation JCL.

Follow these steps:

1. At the ISPF/PDF TSO Command Shell prompt, execute the following command:

```
EXEC 'dsnpref.NMC1.CC2DJCL(INSTALL)'
```

The Install Utility panel appears.

Note: On each of the Install Utility panels, you can use the following keys:

- Enter to proceed to the next panel
- F1 to display online help
- F3 to return to the previous panel
- F4 to exit and return to the main menu

2. Press Enter.

The Install Utility Primary Menu panel appears.

3. Enter **1** (Set Installation Parameters).

The Software Delivery Method panel appears.

4. Complete each of the panels as they open. Press Enter at the completion of each panel.

You must complete all five parameter panels before you can install the product. You can take the default options or specify site-specific values.

Note: For information about the fields, press F1 (Help).

5. Enter **2** (Install Products).

The INSTALLATION Primary Menu panel appears.

6. Enter **1** (Select Products to Install).

The INSTALLATION Product Selection panel appears with previously installed products unavailable.

7. Enter **S** next to the product name and press Enter.

The INSTALLATION Product Confirmation panel appears, confirming your selections.

If you have already installed another product in the product family, the INSTALLATION Components Already Installed panel appears, confirming your selections.

Note: You can enter S next to multiple products to install multiple products at one time. You must be licensed for any products you install.

8. Press Enter to confirm your selection, and complete each of the INSTALLATION panels as they open.

You must complete all the panels before you can set up your regions. You can take the default options or specify site-specific values.

9. Record the data set name into which the JCL was generated in your [post-installation worksheet](#) (see page 175).

You can submit the jobs from the panel or directly from this data set after exiting the panel.

10. Submit and run the following installation jobs in sequence. Do not proceed with any job until the previous job has completed successfully.

I01ALLOC

Allocates the data sets.

The I01ALLOC member allocates CC2DLOAD as a load library of the PDS type. Do not change it to a PDS/E type because the type is not supported.

I02INSMP

Initializes the SMP/E data sets.

I03RCSMP

Performs an SMP/E RECEIVE.

I04AKSMP

Performs an SMP/E APPLY CHECK. This job is listed only if maintenance exists for previously installed products.

I05RSSMP

Performs an SMP/E RESTORE. This job is listed only if maintenance exists for previously installed products.

I06APSMP

Performs an SMP/E APPLY.

I07ACSMP

Performs an SMP/E ACCEPT.

11. If you selected SSL Support as an additional feature to install, the following jobs are also generated. Submit and run them in sequence as for the previous jobs.

- I21ALLME
- I22INIME
- I23RECME
- I26APPMME
- I27ACCME

Notes:

- If you installed and set up your regions without SSL support, and then later install SSL support, add the installed *dsnpref.NMC1.CC2DPLD* data set to the region's STEPLIB or in the system LNKLIST.
- You must have SMP/E V3R5.0 to implement SSL.

12. Press F3.

You are returned to the Primary Menu panel.

Clean Up the USS Directory

Important! This procedure is optional. Do not use this procedure until you complete the entire installation process.

To free file system disk space for subsequent downloads after downloading and processing the pax files for your CA Technologies product, we recommend removing the files from your USS directory and deleting unnecessary MVS data sets. You can delete the following items:

- Pax file
- Product-specific directory created by the pax command and all of the files in it
- SMP/E RELFILES, SMPMCS, and HOLDDATA MVS data sets

These data sets have the HLQ that you assigned in the UNZIPJCL job.

Note: Retain non-SMP/E installation data sets such as *yourHLQ.INSTALL.NOTES* for future reference.

Follow these steps:

1. Navigate to your Pax-Enhanced ESD USS directory.

Your view is of the applicable USS directory.

2. Delete the pax file by entering the following command:

```
rm paxfile
```

paxfile

Specifies the name of the CA Technologies pax file that you downloaded.

The pax file is deleted.

3. Delete the product-specific directory by entering the following command:

```
rm -r product-specific-directory
```

product-specific-directory

Specifies the product-specific directory created by the pax command.

The product-specific directory is deleted.

Note: You can also use TSO ISHELL to navigate to the pax file and product-specific directory, and delete them using the D line command.

Maintenance

Maintenance includes program temporary fixes (PTFs) that supersede all authorized program analysis reports (APARs) that were created up to that time. Details of the superseded APARs are available as comments within the PTFs.

Product Maintenance

Important! The *dsnpref.NMC1.CC2DLINK* data set must be in your system LNKLIST before you start maintenance. You can also create a STEPLIB to the data set name (DSN) in your TSOPROC (that is, allocate it to ISPLLIB). If you installed the product using CA MSM, you must use CA MSM to apply maintenance.

Product maintenance is provided as system modification program (SMP) fixes. The fixes consist of PTFs applied using the IBM System Modification Program Extended (SMP/E) tool.

Note: If an installed SMP fix contains maintenance for the VSAM data sets, you must update those data sets for each region you have set up.

RAMDB maintenance is provided as SMP/E PTFs. However, this is only the delivery and recordkeeping methodology. You must apply the maintenance using \$RMDB04D.

Apply Maintenance

This section describes how to apply individual SMP fixes using the Install Utility.

Note: Individual SMP fixes are only available from the [CA Technical Support site](#) (see page 4).

When you receive SMP fixes, unload them into one of the following:

- A sequential data set
- A member of a partitioned data set

Multiple SMP fixes can be appended into a single data set or member.

Follow these steps:

1. Access the ISPF/PDF Primary Menu.
2. Select the COMMAND option.
The ISPF Command Shell panel appears.
3. At the command prompt, enter the following command:

```
EXEC 'dsnpref.NMC1.CC2DJCL(INSTALL)'
```
4. At the Install Utility title panel, press Enter.
The Install Utility Primary Menu panel appears.
5. At the Install Utility Primary Menu panel, enter **8** (Maintain Products).
The MAINTENANCE Primary Menu panel appears.
6. Enter **3** (Apply individual SMP fixes from a DASD data set).
The MAINTENANCE DASD Fixes Dataset Name panel appears.
7. Enter the data set name that contains the SMP fixes to be applied and press Enter.
8. Complete the fields on the following MAINTENANCE panels as they open.

9. At the MAINTENANCE JCL Library Creation panel, review your fix JCL library.

The default library name is:

dsnpref.NMC1.FIX.DASD.JCL

dsnpref

The same data set prefix you used for the *dsnpref.NMC1.CC2DJCL* data set.

Note: Each time you apply maintenance, use a new output data set. A new data set ensures that the only jobs in your maintenance JCL library are the jobs required for the maintenance you are installing now. To use a new data set:

- Delete the library by issuing a TSO DELETE command and the library name, at the command prompt.
- Specify a new data set name.

10. Press Enter to proceed with the generation of the maintenance JCL.

When the JCL generation is complete, a list of generated jobs and a description of what each member does appears.

11. Note the name of the data set into which the JCL was generated.

12. Submit and run the following jobs in sequence. Do not proceed with any job until the previous job has completed successfully.

Each job must complete with return code 0 unless otherwise indicated.

Important! If there is maintenance for additional features, the SMP/E apply job must be run on a system that has the z/OS UNIX file system used during installation and mounted for read/write access.

F11RCSMP

SMP/E receives maintenance and lists existing HOLDDATA and SOURCEIDs that are already applied. If a job step returns condition code 04, there is no HOLDDATA present.

Review the information. For any held APARs that you want to apply, add the correct BYPASS HOLDx operands to the corresponding APPLY control statement for those APARs. Add the operands by manually editing the F12APSMP job that contains the SMP control statements.

Note: For information about the BYPASS HOLDx operands, see IBM's *SMP/E Commands* guide.

F12APSMP

SMP/E applies maintenance.

13. Press F3.

The Install Utility Primary Menu panel appears.

If the fix contains maintenance for VSAM data sets (as indicated by HOLDDATA), continue with the procedure to update the VSAM data sets for the regions you have set up. Otherwise, you have finished applying the fix.

HOLDDATA

When you apply maintenance, you typically encounter SMP/E HOLDDATA. We use HOLDDATA to notify your SMP/E system of SYSMODs that have errors or special conditions. We support system and external HOLDDATA.

System HOLDDATA

System HOLDDATA indicates data that is an in-stream part of the SYSMOD, informing you of special conditions. The following reasons are used with SYSTEM HOLDDATA for CA NetMaster NM for TCP/IP:

ACTION

Indicates that you must perform special processing before or after you apply this SYSMOD.

AO

Affects automated operations. It changes either the message identifier or the displacement of a field inside the message.

DB2BIND

Indicates that DBRMs have changed and packages need to be rebound.

DDDEF

Indicates that data sets and DDDEFs are being added or modified.

DELETE

Deletes the SYSMOD load module. You cannot reverse this type of SYSMOD with the SMP/E RESTORE command.

DEP

Indicates a dependency for this SYSMOD that you must externally verify.

DOC

Indicates a documentation change with this SYSMOD.

DYNACT

Describes the steps to dynamically activate this fix without performing an IPL.

ENH

Introduces a small programming enhancement. The hold contains the instructions to implement the enhancement. If no action is needed to implement the enhancement, give a summary of the enhancement.

EXIT

Indicates that changes delivered by this SYSMOD require reassembly of user exits.

EXRF

Indicates that the SYSMOD must be installed in both the Active and Alternate Extended Recovery Facility Systems.

MULTSYS

Apply this SYSMOD to multiple systems for either pre-conditioning, coexistence, or exploitation.

RESTART

Indicates that after applying this SYSMOD, the site must perform a special restart as opposed to a routine restart.

SYSMOD

Indicates that some or all of the elements delivered by this SYSMOD are to be downloaded to a workstation.

Code a bypass operand on your APPLY command to install SYSMODs that have internal holds. Code the bypass operand only after you have performed the required action, or if you are performing the action after the APPLY, if that is appropriate.

External HOLDDATA

External HOLDDATA is not part of the PTF. It resides in a separate file. It is commonly used for SYSMODs that have been distributed and later are discovered to cause problems.

Download the external HOLDDATA from CA Support to a DASD file, and allocate the file to the SMPHOLD DD statement. To take care of the external HOLDDATA, receive it into your SMP/E environment. SMP/E receives the HOLDDATA from CA-supplied jobs.

If a SYSMOD has an unresolved hold error, SMP/E does not install it unless you add a bypass to your APPLY command. You can bypass an error hold in situations that are not applicable to you. Error holds that are not applicable to you can include a problem that happens only with a hardware device that you do not have or in a product feature that you do not use.

When CA publishes a SYSMOD that resolves the hold, the resolving SYSMOD supersedes the hold error. This action lets you apply the original SYSMOD in conjunction with the fixing SYSMOD.

A special HOLDDATA class called ERREL exists. We have determined that the problem fixed by the SYSMOD is more important than the one that it causes. We recommend that you apply these SYSMODs.

The only manual task is running a REPORT ERRSYSMODS. This report identifies the following:

- Any held SYSMODs already applied to your system.
- Any resolving SYSMODs that are in RECEIVE status.

SMP/E identifies the SYSMOD to apply to correct the situation.

Update VSAM Data Sets

If an installed SMP fix contains maintenance for the VSAM data sets, maintenance option V of the Install Utility becomes available. To complete maintenance, select the option to update the data sets for the regions you have set up.

Follow these steps:

1. Access the ISPF/PDF Primary Menu, and select the COMMAND option.
The ISPF Command Shell panel appears.
2. At the command prompt, execute the following command:

```
EXEC 'dsnpref.NMC1.CC2DJCL(INSTALL)'
```


The Install Utility title panel appears.
3. Press Enter.
The Install Utility Primary Menu panel appears.
4. Enter **8** (Maintain Products).
The MAINTENANCE Primary Menu panel appears.
5. Enter **V** (Update MODS, PANELS, OSCNTL and NETINFO data sets with installed maintenance).
The MAINTENANCE Shared Region Data Sets panel appears.
6. Review the information, and press Enter.
7. At the MAINTENANCE JOBCARD Information panel, specify your JOBCARD details and press Enter.

8. At the MAINTENANCE JCL Library Creation panel, review your fix JCL library. The default library name is:

dsnpref.NMC1.FIX.VSAMUPD.JCL

dsnpref

The same data set prefix used for the *dsnpref.NMC1.CC2DJCL* data set.

Note: Each time you apply maintenance, use a new output data set. The new data set helps ensure that the only jobs in your maintenance JCL library are the jobs required for the maintenance you are installing. To use a new data set, take *one* of the following actions:

- Delete the library by issuing a TSO DELETE command and the library name, at the command prompt.
- Specify a new data set name.

9. Press Enter to proceed with the generation of the maintenance JCL.

10. Submit and run the job F21RFRSH to update the VSAM data sets.

Note: The utility also generates the following jobs: F22DUMP and F23REST. If a shared DASD is not available, the jobs help you deploy those updates to a target system. The F22DUMP job creates backup data set that include the updated VSAM data sets, which you deploy to the target system. This backup data set is *dsnpref.DFDSS.SHARED*. The F23REST job, when submitted on the target system, restores the updated VSAM data sets from the backup data sets.

11. Press F3.

The Install Utility Primary Menu panel appears.

12. Press F4 to exit the Install Utility Primary Menu panel and return to the ISPF Command Shell panel, or continue with the other options.

Individual RAMDB Maintenance

Note: Individual RAMDB maintenance is also available from the [CA Technical Support site](#) (see page 4).

This section describes how to apply maintenance to the RAMDB and details the command syntax of the \$RMDB04D maintenance utility. You apply this maintenance in an active region.

Important! The RAMDB data set must not be updated with individual replacement records using the IDCAMS REPRO command.

You use [\\$RMDB04D OPT=APPLY](#) (see page 66) to apply maintenance. When applying maintenance, you can use the DIFF operand to display details of what differences are being added, replaced, or deleted by the maintenance.

Create Backup RAMDB

As a safety precaution, create a backup of your RAMDB (herein referred to RAMDBd) before applying maintenance.

Follow these steps:

1. Allocate RAMDBd in the same way that RAMDB was allocated.
The cluster definition is in *dsnpref.NMC1.rname.JCL(S01LCALC)*.
2. Stop the product region.
3. Copy the data from RAMDB to RAMDBd using IDCAMS REPRO command.
Note: For information, see the example in *dsnpref.NMC1.rname.JCL(S04LDVSM)*.
4. Restart the product region.

Apply Maintenance to RAMDB

You can apply maintenance directly to your RAMDB. The maintenance can then propagate to all connected regions, if any. If necessary, you can restore the maintenance using your RAMDBd as input (if the maintenance has not yet been applied to RAMDBd).

Follow these steps:

1. Log on to your product region and enter CMD.
The command entry panel appears.
2. Apply-check the RAMDB fix by entering the following command:

```
$RMDB04D OPT=APPLY FIX=fix-name CHECK=YES
```

fix_name

Is RAM@UPDT for published solutions or TZdddd for test fixes.

When the APPLY CHECK finishes, a report appears. The report shows whether an APPLY of the fix will be successful, and also exactly what changes will result from the APPLY.

Note: Perform this step for the following reasons:

- To see what happens if a fix is applied to a RAMDB
 - To see whether a fix has been applied to a RAMDB
3. Apply the RAMDB fix by entering the following command:

```
$RMDB04D OPT=APPLY FIX=fix_name
```

Note: If a RAMDB fix does not apply correctly or if you want to restore a fix, [restore the RAMDB maintenance](#) (see page 66).

Restore RAMDB Maintenance

Note: This step is optional.

The RESTORE option can be used to remove an applied fix from the RAMDB by using RAMDBd as input. The fix is effectively reversed, that is, any added objects are deleted and any deleted or replaced objects are copied from RAMDBd back to the RAMDB.

To restore the fix, enter the following command:

```
$RMDB04D OPT=RESTORE FIX=fix_name DDBDSN=?RAMDBd-dataset-name DDB=?RAMDBd
```

?*RAMDBd*

Specifies the ddname for the backup RAMDB.

?*RAMDBd-dataset-name*

Specifies the full data set name of the backup RAMDB.

RAMDB Maintenance Utility Syntax

This section describes the syntax of the RAMDB maintenance utility.

\$RMDB04D OPT=APPLY

Use this procedure to apply a fix to a RAMDB or check a fix against a RAMDB.

This procedure has the following format:

```
$RMDB04D OPT=APPLY  
      FIX=fix-number  
      [DDNAME=ddname | DATASET=dataset-name]  
      [CHECK={NO | YES}]  
      [DIFF={YES | NO}]  
      [FORCE={NO | YES}]  
      [CONFIRM={YES | NO}]  
      [DB=file-id [DBDSN=db-dataset-name]]
```

OPT=APPLY

Specifies that a fix is being applied to a RAMDB.

FIX=*fix-number*

Specifies the fix number. This number is used as the member name of the input partitioned data set.

[DDNAME=*ddname* | DATASET=*dataset-name*]

Specifies the DDNAME parameter if the data set containing the fix is already allocated to the system, or the DATASET parameter if the data set containing the fix is to be allocated and freed after the fix has been retrieved. These two parameters are mutually exclusive and, therefore, you cannot specify both of them. If neither is specified, the COMMANDS DD concatenation in the region is used.

[CHECK={NO | YES}]

Specifies whether the fix is checked. If you specify YES, the fix is checked only for compatibility with the database and is not applied to the database. The check phase is always performed regardless of the value specified. However, this parameter determines whether the check phase is the only phase to be performed.

[DIFF={YES | NO}]

Specifies whether differences are displayed. If you specify YES (the default), the differences between the target objects and the new objects contained in the fix are displayed for each updated object. This applies to any SET (update) and CREATE (add) actions in the fix member where the target objects already exist.

[FORCE={NO | YES}]

Specifies whether the fix is applied regardless of the success or failure of the check phase. However, if CHECK=YES is specified, the FORCE parameter has no effect.

[CONFIRM={YES | NO}]

Specifies whether the fix is retrieved and the syntax checked before being presented as a panel for browsing. The panel enables you to view the fix and confirm the application. After you confirm, the fix is applied, and the message log displays another panel for browsing. If you specify NO, the fix is applied without presenting any confirmation panel and the message log is written to the terminal rather than being displayed as a panel.

The message log is always written to the activity log regardless of the options specified.

[DB=*file-id* [DBDSN=*db-dataset-name*]]

Specifies the DB parameter to apply the fix to a database other than the currently allocated RAMDB. This parameter specifies the file ID of the target database. If you also specify the DBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the fix is applied. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

\$RMDB04D OPT=RESTORE

Use this procedure to reverse the effect of a fix.

This procedure has the following format:

```
$RMDB04D OPT=RESTORE
      FIX=fix-number
      [DDNAME=ddname | DATASET=dataset-name]
      [CONFIRM={YES | NO}]
      [TDB=target-file-id [TDBDSN=target-dataset-name]]
      [DDB=source-file-id [DDBDSN=source-dataset-name]]
```

OPT=RESTORE

Specifies that a fix, which has been applied to the target RAMDB, is being reversed.

FIX= *fix-number*

Specifies the fix number to back out of the RAMDB. This number is used as the member name of the fix data set and is verified against the contents of the member for the correct fix.

[DDNAME=*ddname* | DATASET=*dataset-name*]

Specifies the DDNAME parameter if the data set containing the fix is already allocated to the system, or the DATASET parameter if the data set containing the fix is to be allocated and freed after the fix has been retrieved. These two parameters are mutually exclusive and, therefore, you cannot specify both of them. If neither is specified, the COMMANDS DD concatenation in the region is used.

[CONFIRM={YES | NO}]

Specifies whether the fix is retrieved and the syntax checked before being presented as a panel for browsing. The panel lets you view the fix and confirm the restoration process. After you confirm, the fix is removed and the original data restored. The message log is presented as another panel for browsing. If you specify NO, the restoration process proceeds without presenting any confirmation panel, and the message log is written to the terminal rather than being displayed as a panel.

The message log is always written to the activity log regardless of the options specified.

[TDB=*target-file-id* [TDBDSN=*target-dataset-name*]]

Reverses a fix in a database other than the currently allocated RAMDB. This parameter specifies the file ID of the target database. If you also specify the TDBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the restoration process. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

DDB=source-file-id [DDBDSN=source-dataset-name]

Specifies the file ID of the source database.

Note: Restoration requires the specification of the distribution (source) database through the DDB parameter.

The source database must be a copy of the original database. If you also specify the DDBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the restoration process. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

Chapter 5: Installing Your Product from Tape

This section contains the following topics:

[Unload the Install Utility](#) (see page 71)

[Installation JCL](#) (see page 74)

[Maintenance](#) (see page 77)

Unload the Install Utility

The installation utility software lets you generate and run the JCL required to install your product. The installation utility software is delivered on tape.

The installation software unloads into the *dsnpref.NMC1.CC2DJCL* data set; *dsnpref* is a prefix you specify for your product data sets.

To unload the install utility, do *one* of the following:

- If *dsnpref.NMC1.CC2DJCL* does not exist and you are installing from tape, [unload into a new data set from tape](#) (see page 71).
- If *dsnpref.NMC1.CC2DJCL* exists from a previous installation and you are installing from tape at the current release level, [unload into an existing data set from tape](#) (see page 73).

Additional Features

The Install Utility provides an option to install the following additional features:

- SSL support
- ReportCenter

Install, set up, and customize your product region completely before installing ReportCenter.

Note: For information about installing these features, see the *ReportCenter Guide*.

Unload into a New Data Set from Tape

If *dsnpref.NMC1.CC2DJCL* does not exist and you are installing from tape, you must unload the installation software from tape on to your DASD and into a new data set.

Follow these steps:

1. Create an unload job by copying the following JCL:

```
//jobname JOB .....
//STEP1 EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//SYSUT1 DD DSN=CAI.SAMPJCL,
//          DISP=OLD,UNIT=?device-in,VOL=SER=?tapeser,
//          LABEL=(1,SL,EXPDT=98000)
//SYSUT2 DD DSN=?dsnpref.NMC1.CC2DJCL,
//          DISP=(NEW,CATLG,DELETE),
//          UNIT=?device-out,VOL=SER=?volser,
//          SPACE=(CYL,(10,1,140)),
//          DCB=(RECFM=FB,LRECL=80,BLKSIZE=0)
//SYSIN DD DUMMY
```

Important! The SYSUT2 data set name must end with NMC1.CC2DJCL.

2. Replace the statements prefixed with a question mark (?) with your own values as follows:

?device-in

Specifies the tape drive unit to mount the tape.

?tapeser

Specifies the tape volume serial number in the form C2D76x. The value for this release is C2D760.

?dsnpref

Specifies the data set prefix that will be used for the installation, maintenance, and Install Utility data sets. Do not include the name of your planned product region in the prefix; *?dsnpref* can be up to 29 characters long. If the data set high level qualifiers you are using do not exist, define an alias entry in the master catalog.

?device-out

Specifies the type of the DASD device where you want to place the installation software.

?volser

Specifies the volume serial number of the DASD.

If allocation is controlled by SMS, replace UNIT= and VOL=SER= with STORCLAS=?storclass.

3. Submit and run the job.
4. Check that the job successfully completed.

Unload into an Existing Data Set from Tape

If *dsnpref.NMC1.CC2DJCL* exists from a previous installation at the current release level, unload the installation software from tape into the existing data set.

Follow these steps:

1. Create an unload job by copying the following JCL:

```
//jobname JOB .....
//STEP1 EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//SYSUT1 DD DSN=CAI.SAMPJCL,
//          DISP=OLD,UNIT=?device-in,VOL=SER=?tapeser,
//          LABEL=(1,SL,EXPDT=98000)
//SYSUT2 DD DSN=?dsnpref.NMC1.CC2DJCL,
//          DISP=OLD
//SYSIN DD *
        COPY I=((SYSUT1,R)),0=SYSUT2
        COPY I=((SYSUT2,R)),0=SYSUT2
/*
```

2. Replace the statements prefixed with a question mark (?) with your own values as follows:

?device-in

Specifies the tape drive unit to mount the tape.

?tapeser

Specifies the tape volume serial number in the form C2D76x. The value for this release is C2D760.

?dsnpref

Specifies the data set prefix in the previous installation.

3. Submit and run the job.
4. Verify that the job successfully completed.

Installation JCL

The installation process creates the *dsnpref*.NMC1.INSTDB database to store details of each installation that you perform. If you are also installing other products in the CA Mainframe Network Management family of products, this database manages those installations. These details include the products you install and the installation values that you specify.

Note: During this task, the INSTALLATION JCL Library Creation panel lets you specify your installation JCL library. The default library name is *dsnpref*.NMC1.INSTALL.JCL, where *dsnpref* is the same data set prefix you used for the *dsnpref*.NMC1.CC2DJCL data set.

If your installation JCL library exists, do *one* of the following:

- Specify a new data set name at that panel.
- Delete the existing library by issuing a TSO DELETE command.

Note: If you leave the Install Utility at any stage, you can return to it from the ISPF/PDF TSO Command Shell prompt. Execute the following command:

```
EXEC 'dsnpref.NMC1.CC2DJCL(INSTALL)'
```

Generate the Installation JCL

During the installation process, you provide the [site-specific installation information that you previously collected](#) (see page 163). This information is used to generate the installation JCL.

Follow these steps:

1. At the ISPF/PDF TSO Command Shell prompt, execute the following command:

```
EXEC 'dsnpref.NMC1.CC2DJCL(INSTALL)'
```

The Install Utility panel appears.

Note: On each of the Install Utility panels, you can use the following keys:

- Enter to proceed to the next panel
 - F1 to display online help
 - F3 to return to the previous panel
 - F4 to exit and return to the main menu
2. Press Enter.
The Install Utility Primary Menu panel appears.

3. Enter **1** (Set Installation Parameters).

The Software Delivery Method panel appears.

4. Complete each of the panels as they open. Press Enter at the completion of each panel.

You must complete all five parameter panels before you can install the product. You can take the default options or specify site-specific values.

Note: For information about the fields, press F1 (Help).

5. Enter **2** (Install Products).

The INSTALLATION Primary Menu panel appears.

6. Enter **1** (Select Products to Install).

The INSTALLATION Product Selection panel appears with previously installed products unavailable.

7. Enter **S** next to the product name and press Enter.

The INSTALLATION Product Confirmation panel appears, confirming your selections.

If you have already installed another product in the product family, the INSTALLATION Components Already Installed panel appears, confirming your selections.

Note: You can enter S next to multiple products to install multiple products at one time. You must be licensed for any products you install.

8. Press Enter to confirm your selection, and complete each of the INSTALLATION panels as they open.

You must complete all the panels before you can set up your regions. You can take the default options or specify site-specific values.

9. Record the data set name into which the JCL was generated in your [post-installation worksheet](#) (see page 175).

You can submit the jobs from the panel or directly from this data set after exiting the panel.

10. Submit and run the following installation jobs in sequence. Do not proceed with any job until the previous job has completed successfully.

I01ALLOC

Allocates the data sets.

The I01ALLOC member allocates CC2DLOAD as a load library of the PDS type. Do not change it to a PDS/E type because the type is not supported.

I02INSMP

Initializes the SMP/E data sets.

I03RCSMP

Performs an SMP/E RECEIVE.

I04AKSMP

Performs an SMP/E APPLY CHECK. This job is listed only if maintenance exists for previously installed products.

I05RSSMP

Performs an SMP/E RESTORE. This job is listed only if maintenance exists for previously installed products.

I06APSMP

Performs an SMP/E APPLY.

I07ACSMP

Performs an SMP/E ACCEPT.

11. If you selected SSL Support as an additional feature to install, the following jobs are also generated. Submit and run them in sequence as for the previous jobs.

- I21ALLME
- I22INIME
- I23RECME
- I26APPME
- I27ACCME

Notes:

- If you installed and set up your regions without SSL support, and then later install SSL support, add the installed *dsnpref.NMC1.CC2DPLD* data set to the region's STEPLIB or in the system LNKST.
- You must have SMP/E V3R5.0 to implement SSL.

12. Press F3.

You are returned to the Primary Menu panel.

Maintenance

Maintenance includes program temporary fixes (PTFs) that supersede all authorized program analysis reports (APARs) that were created up to that time. Details of the superseded APARs are available as comments within the PTFs.

Product Maintenance

Important! The *dsnpref.NMC1.CC2DLINK* data set must be in your system LNKST before you start maintenance. You can also create a STEPLIB to the data set name (DSN) in your TSOPROC (that is, allocate it to ISPLLIB). If you installed the product using CA MSM, you must use CA MSM to apply maintenance.

Product maintenance is provided as system modification program (SMP) fixes. The fixes consist of PTFs applied using the IBM System Modification Program Extended (SMP/E) tool.

Note: If an installed SMP fix contains maintenance for the VSAM data sets, you must update those data sets for each region you have set up.

RAMDB maintenance is provided as SMP/E PTFs. However, this is only the delivery and recordkeeping methodology. You must apply the maintenance using \$RMDB04D.

Apply Maintenance

This section describes how to apply individual SMP fixes using the Install Utility.

Note: Individual SMP fixes are only available from the [CA Technical Support site](#) (see page 4).

When you receive SMP fixes, unload them into one of the following:

- A sequential data set
- A member of a partitioned data set

Multiple SMP fixes can be appended into a single data set or member.

Follow these steps:

1. Access the ISPF/PDF Primary Menu.
2. Select the COMMAND option.
The ISPF Command Shell panel appears.
3. At the command prompt, enter the following command:
`EXEC 'dsnpref.NMC1.CC2DJCL(INSTALL)'`
4. At the Install Utility title panel, press Enter.
The Install Utility Primary Menu panel appears.
5. At the Install Utility Primary Menu panel, enter **8** (Maintain Products).
The MAINTENANCE Primary Menu panel appears.
6. Enter **3** (Apply individual SMP fixes from a DASD data set).
The MAINTENANCE DASD Fixes Dataset Name panel appears.
7. Enter the data set name that contains the SMP fixes to be applied and press Enter.
8. Complete the fields on the following MAINTENANCE panels as they open.
9. At the MAINTENANCE JCL Library Creation panel, review your fix JCL library.
The default library name is:
`dsnpref.NMC1.FIX.DASD.JCL`
dsnpref
The same data set prefix you used for the *dsnpref.NMC1.CC2DJCL* data set.
Note: Each time you apply maintenance, use a new output data set. A new data set ensures that the only jobs in your maintenance JCL library are the jobs required for the maintenance you are installing now. To use a new data set:
 - Delete the library by issuing a TSO DELETE command and the library name, at the command prompt.
 - Specify a new data set name.
10. Press Enter to proceed with the generation of the maintenance JCL.
When the JCL generation is complete, a list of generated jobs and a description of what each member does appears.
11. Note the name of the data set into which the JCL was generated.

12. Submit and run the following jobs in sequence. Do not proceed with any job until the previous job has completed successfully.

Each job must complete with return code 0 unless otherwise indicated.

Important! If there is maintenance for additional features, the SMP/E apply job must be run on a system that has the z/OS UNIX file system used during installation and mounted for read/write access.

F11RCSMP

SMP/E receives maintenance and lists existing HOLDDATA and SOURCEIDs that are already applied. If a job step returns condition code 04, there is no HOLDDATA present.

Review the information. For any held APARs that you want to apply, add the correct BYPASS HOLDx operands to the corresponding APPLY control statement for those APARs. Add the operands by manually editing the F12APSMP job that contains the SMP control statements.

Note: For information about the BYPASS HOLDx operands, see IBM's *SMP/E Commands* guide.

F12APSMP

SMP/E applies maintenance.

13. Press F3.

The Install Utility Primary Menu panel appears.

If the fix contains maintenance for VSAM data sets (as indicated by HOLDDATA), continue with the procedure to update the VSAM data sets for the regions you have set up. Otherwise, you have finished applying the fix.

HOLDDATA

When you apply maintenance, you typically encounter SMP/E HOLDDATA. We use HOLDDATA to notify your SMP/E system of SYSMODs that have errors or special conditions. We support system and external HOLDDATA.

System HOLDDATA

System HOLDDATA indicates data that is an in-stream part of the SYSMOD, informing you of special conditions. The following reasons are used with SYSTEM HOLDDATA for CA NetMaster NM for TCP/IP:

ACTION

Indicates that you must perform special processing before or after you apply this SYSMOD.

AO

Affects automated operations. It changes either the message identifier or the displacement of a field inside the message.

DB2BIND

Indicates that DBRMs have changed and packages need to be rebound.

DDDEF

Indicates that data sets and DDDEFs are being added or modified.

DELETE

Deletes the SYSMOD load module. You cannot reverse this type of SYSMOD with the SMP/E RESTORE command.

DEP

Indicates a dependency for this SYSMOD that you must externally verify.

DOC

Indicates a documentation change with this SYSMOD.

DYNACT

Describes the steps to dynamically activate this fix without performing an IPL.

ENH

Introduces a small programming enhancement. The hold contains the instructions to implement the enhancement. If no action is needed to implement the enhancement, give a summary of the enhancement.

EXIT

Indicates that changes delivered by this SYSMOD require reassembly of user exits.

EXRF

Indicates that the SYSMOD must be installed in both the Active and Alternate Extended Recovery Facility Systems.

MULTSYS

Apply this SYSMOD to multiple systems for either pre-conditioning, coexistence, or exploitation.

RESTART

Indicates that after applying this SYSMOD, the site must perform a special restart as opposed to a routine restart.

SYSMOD

Indicates that some or all of the elements delivered by this SYSMOD are to be downloaded to a workstation.

Code a bypass operand on your APPLY command to install SYSMODs that have internal holds. Code the bypass operand only after you have performed the required action, or if you are performing the action after the APPLY, if that is appropriate.

External HOLDDATA

External HOLDDATA is not part of the PTF. It resides in a separate file. It is commonly used for SYSMODs that have been distributed and later are discovered to cause problems.

Download the external HOLDDATA from CA Support to a DASD file, and allocate the file to the SMPHOLD DD statement. To take care of the external HOLDDATA, receive it into your SMP/E environment. SMP/E receives the HOLDDATA from CA-supplied jobs.

If a SYSMOD has an unresolved hold error, SMP/E does not install it unless you add a bypass to your APPLY command. You can bypass an error hold in situations that are not applicable to you. Error holds that are not applicable to you can include a problem that happens only with a hardware device that you do not have or in a product feature that you do not use.

When CA publishes a SYSMOD that resolves the hold, the resolving SYSMOD supersedes the hold error. This action lets you apply the original SYSMOD in conjunction with the fixing SYSMOD.

A special HOLDDATA class called ERREL exists. We have determined that the problem fixed by the SYSMOD is more important than the one that it causes. We recommend that you apply these SYSMODs.

The only manual task is running a REPORT ERRSYSMODS. This report identifies the following:

- Any held SYSMODs already applied to your system.
- Any resolving SYSMODs that are in RECEIVE status.

SMP/E identifies the SYSMOD to apply to correct the situation.

Update VSAM Data Sets

If an installed SMP fix contains maintenance for the VSAM data sets, maintenance option V of the Install Utility becomes available. To complete maintenance, select the option to update the data sets for the regions you have set up.

Follow these steps:

1. Access the ISPF/PDF Primary Menu, and select the COMMAND option.

The ISPF Command Shell panel appears.

2. At the command prompt, execute the following command:

```
EXEC 'dsnpref.NMC1.CC2DJCL(INSTALL)'
```

The Install Utility title panel appears.

3. Press Enter.

The Install Utility Primary Menu panel appears.

4. Enter **8** (Maintain Products).

The MAINTENANCE Primary Menu panel appears.

5. Enter **V** (Update MODS, PANELS, OSCNTL and NETINFO data sets with installed maintenance).

The MAINTENANCE Shared Region Data Sets panel appears.

6. Review the information, and press Enter.

7. At the MAINTENANCE JOBCARD Information panel, specify your JOBCARD details and press Enter.

8. At the MAINTENANCE JCL Library Creation panel, review your fix JCL library. The default library name is:

dsnpref.NMC1.FIX.VSAMUPD.JCL

dsnpref

The same data set prefix used for the *dsnpref.NMC1.CC2DJCL* data set.

Note: Each time you apply maintenance, use a new output data set. The new data set helps ensure that the only jobs in your maintenance JCL library are the jobs required for the maintenance you are installing. To use a new data set, take *one* of the following actions:

- Delete the library by issuing a TSO DELETE command and the library name, at the command prompt.
- Specify a new data set name.

9. Press Enter to proceed with the generation of the maintenance JCL.

10. Submit and run the job F21RFRSH to update the VSAM data sets.

Note: The utility also generates the following jobs: F22DUMP and F23REST. If a shared DASD is not available, the jobs help you deploy those updates to a target system. The F22DUMP job creates backup data set that include the updated VSAM data sets, which you deploy to the target system. This backup data set is *dsnpref.DFDSS.SHARED*. The F23REST job, when submitted on the target system, restores the updated VSAM data sets from the backup data sets.

11. Press F3.

The Install Utility Primary Menu panel appears.

12. Press F4 to exit the Install Utility Primary Menu panel and return to the ISPF Command Shell panel, or continue with the other options.

Individual RAMDB Maintenance

Note: Individual RAMDB maintenance is also available from the [CA Technical Support site](#) (see page 4).

This section describes how to apply maintenance to the RAMDB and details the command syntax of the \$RMDB04D maintenance utility. You apply this maintenance in an active region.

Important! The RAMDB data set must not be updated with individual replacement records using the IDCAMS REPRO command.

You use [\\$RMDB04D OPT=APPLY](#) (see page 66) to apply maintenance. When applying maintenance, you can use the DIFF operand to display details of what differences are being added, replaced, or deleted by the maintenance.

Create Backup RAMDB

As a safety precaution, create a backup of your RAMDB (herein referred to RAMDBd) before applying maintenance.

Follow these steps:

1. Allocate RAMDBd in the same way that RAMDB was allocated.
The cluster definition is in *dsnpref.NMC1.rname.JCL(S01LCALC)*.
2. Stop the product region.
3. Copy the data from RAMDB to RAMDBd using IDCAMS REPRO command.
Note: For information, see the example in *dsnpref.NMC1.rname.JCL(S04LDVSM)*.
4. Restart the product region.

Apply Maintenance to RAMDB

You can apply maintenance directly to your RAMDB. The maintenance can then propagate to all connected regions, if any. If necessary, you can restore the maintenance using your RAMDBd as input (if the maintenance has not yet been applied to RAMDBd).

Follow these steps:

1. Log on to your product region and enter CMD.

The command entry panel appears.

2. Apply-check the RAMDB fix by entering the following command:

```
$RMDB04D OPT=APPLY FIX=fix-name CHECK=YES
```

fix_name

Is RAM@UPDT for published solutions or TZdddd for test fixes.

When the APPLY CHECK finishes, a report appears. The report shows whether an APPLY of the fix will be successful, and also exactly what changes will result from the APPLY.

Note: Perform this step for the following reasons:

- To see what happens if a fix is applied to a RAMDB
- To see whether a fix has been applied to a RAMDB

3. Apply the RAMDB fix by entering the following command:

```
$RMDB04D OPT=APPLY FIX=fix_name
```

Note: If a RAMDB fix does not apply correctly or if you want to restore a fix, [restore the RAMDB maintenance](#) (see page 66).

Restore RAMDB Maintenance

Note: This step is optional.

The RESTORE option can be used to remove an applied fix from the RAMDB by using RAMDBd as input. The fix is effectively reversed, that is, any added objects are deleted and any deleted or replaced objects are copied from RAMDBd back to the RAMDB.

To restore the fix, enter the following command:

```
$RMDB04D OPT=RESTORE FIX=fix_name DDBDSN=?RAMDBd-dataset-name DDB=?RAMDBd
```

?RAMDBd

Specifies the ddname for the backup RAMDB.

?RAMDBd-dataset-name

Specifies the full data set name of the backup RAMDB.

RAMDB Maintenance Utility Syntax

This section describes the syntax of the RAMDB maintenance utility.

\$RMDB04D OPT=APPLY

Use this procedure to apply a fix to a RAMDB or check a fix against a RAMDB.

This procedure has the following format:

```
$RMDB04D OPT=APPLY
      FIX=fix-number
      [DDNAME=ddname | DATASET=dataset-name]
      [CHECK={NO | YES}]
      [DIFF={YES | NO}]
      [FORCE={NO | YES}]
      [CONFIRM={YES | NO}]
      [DB=file-id [DBDSN=db-dataset-name]]
```

OPT=APPLY

Specifies that a fix is being applied to a RAMDB.

FIX=*fix-number*

Specifies the fix number. This number is used as the member name of the input partitioned data set.

[DDNAME=*ddname* | DATASET=*dataset-name*]

Specifies the DDNAME parameter if the data set containing the fix is already allocated to the system, or the DATASET parameter if the data set containing the fix is to be allocated and freed after the fix has been retrieved. These two parameters are mutually exclusive and, therefore, you cannot specify both of them. If neither is specified, the COMMANDS DD concatenation in the region is used.

[CHECK={NO | YES}]

Specifies whether the fix is checked. If you specify YES, the fix is checked only for compatibility with the database and is not applied to the database. The check phase is always performed regardless of the value specified. However, this parameter determines whether the check phase is the only phase to be performed.

[DIFF={YES | NO}]

Specifies whether differences are displayed. If you specify YES (the default), the differences between the target objects and the new objects contained in the fix are displayed for each updated object. This applies to any SET (update) and CREATE (add) actions in the fix member where the target objects already exist.

[FORCE={NO | YES}]

Specifies whether the fix is applied regardless of the success or failure of the check phase. However, if CHECK=YES is specified, the FORCE parameter has no effect.

[CONFIRM={YES | NO}]

Specifies whether the fix is retrieved and the syntax checked before being presented as a panel for browsing. The panel enables you to view the fix and confirm the application. After you confirm, the fix is applied, and the message log displays another panel for browsing. If you specify NO, the fix is applied without presenting any confirmation panel and the message log is written to the terminal rather than being displayed as a panel.

The message log is always written to the activity log regardless of the options specified.

[DB=*file-id* [DBDSN=db-*dataset-name*]]

Specifies the DB parameter to apply the fix to a database other than the currently allocated RAMDB. This parameter specifies the file ID of the target database. If you also specify the DBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the fix is applied. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

\$RMDB04D OPT=RESTORE

Use this procedure to reverse the effect of a fix.

This procedure has the following format:

```
$RMDB04D OPT=RESTORE
      FIX=fix-number
      [DDNAME=ddname | DATASET=dataset-name]
      [CONFIRM={YES | NO}]
      [TDB=target-file-id [TDBDSN=target-dataset-name]]
      [DDB=source-file-id [DDBDSN=source-dataset-name]]
```

OPT=RESTORE

Specifies that a fix, which has been applied to the target RAMDB, is being reversed.

FIX= *fix-number*

Specifies the fix number to back out of the RAMDB. This number is used as the member name of the fix data set and is verified against the contents of the member for the correct fix.

[DDNAME=*ddname* | DATASET=*dataset-name*]

Specifies the DDNAME parameter if the data set containing the fix is already allocated to the system, or the DATASET parameter if the data set containing the fix is to be allocated and freed after the fix has been retrieved. These two parameters are mutually exclusive and, therefore, you cannot specify both of them. If neither is specified, the COMMANDS DD concatenation in the region is used.

[CONFIRM={YES | NO}]

Specifies whether the fix is retrieved and the syntax checked before being presented as a panel for browsing. The panel lets you view the fix and confirm the restoration process. After you confirm, the fix is removed and the original data restored. The message log is presented as another panel for browsing. If you specify NO, the restoration process proceeds without presenting any confirmation panel, and the message log is written to the terminal rather than being displayed as a panel.

The message log is always written to the activity log regardless of the options specified.

[TDB=*target-file-id* [TDBDSN=*target-dataset-name*]]

Reverses a fix in a database other than the currently allocated RAMDB. This parameter specifies the file ID of the target database. If you also specify the TDBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the restoration process. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

[DDB=*source-file-id* [DDBDSN=*source-dataset-name*]]

Specifies the file ID of the source database.

Note: Restoration requires the specification of the distribution (source) database through the DDB parameter.

The source database must be a copy of the original database. If you also specify the DDBDSN parameter, the specified data set is allocated a ddname that is the same as the specified file ID, and is opened and started. The database is not freed after the restoration process. If the database is already allocated, the specified data set name is verified as allocated to the ddname (that is the same as the specified file ID) and opened to the same file ID.

Chapter 6: Configuring Your Product

The topics in this section describe the manual tasks you perform if you are not configuring your product using CA MSM.

You use the Install Utility to set up the regions required by this product.

Important! You must put the *dsnpref.NMC1.CC2DLINK* data set in your system LNKST before you start setting up regions. You can also create a STEPLIB to the data set name (DSN) in your TSOPROC (that is, allocate it to ISPLLIB).

This section contains the following topics:

[How Region Setup Works](#) (see page 89)

[Region Contents](#) (see page 89)

[SOLVE SSI as Common Component](#) (see page 90)

[Specify the SOLVE SSI Region](#) (see page 90)

[Specify the Product Region](#) (see page 92)

How Region Setup Works

You can have more than one region on a system. Each region runs as a started task.

The Install Utility uses the [site-specific information you collected during preinstallation](#) (see page 163) to generate the jobs that build the regions. If you need additional regions, you can reuse the Install Utility to create them.

Important! After you have run a setup job, you cannot alter the results using the setup software. You can use the setup software to create a region, or you can manually customize the JCL for the existing region.

Region Contents

Your product is comprised of the following regions:

SOLVE Subsystem Interface (SOLVE SSI) Region

Provides communication between the product region and other software on a system. One SOLVE SSI can serve multiple product regions.

Product Region

Specifies where you log in and use your product. You can have more than one product region on a system.

SOLVE SSI as Common Component

The SOLVE SSI is a common component for multiple CA product families and can serve multiple product regions on a system. The following methods are available:

- One shared SSI to serve all product families.
- A separate SSI for each product family (CA Mainframe Network Management, CA SOLVE:Operations Automation, and CA SOLVE:Access).
- A mix of the first two methods, for example, CA SOLVE:Access has its own SSI and CA Mainframe Network Management and CA SOLVE:Operations Automation share an SSI.

Note: If you have already installed another Mainframe Network Management product and set up a SOLVE SSI, you do not need to set up another SOLVE SSI. You must, however, ensure that the SOLVE SSI parameters suit your product and site requirements.

Specify the SOLVE SSI Region

Use this procedure to provide communication between the product region and other software on a system.

Follow these steps:

1. At the ISPF/PDF TSO Command Shell prompt, execute the following command:

```
EXEC 'dsnpref.NMC1.CC2DJCL(INSTALL)'
```

The Install Utility panel appears.

Note: On each of the Install Utility panels, you can use the following keys:

- Enter to proceed to the next panel
- F1 to display the online help
- F3 to return to the previous panel
- F4 to exit and return to the main menu

2. Press Enter.

The Install Utility Primary Menu panel appears.

3. (Optional) If you have installed the product using CA MSM, perform the following steps:
 - a. Enter **1**.

The Software Delivery Method panel appears.
 - b. Complete the panel:
 - Enter **S** next to CA MSM.
 - Specify the name of the CSI data set used during product installation in the SMP/E CSI Used field.
 - c. Press Enter.
4. Enter **4**.

A panel appears listing several approaches to implement your SOLVE SSI environment.

Note: For more information, press F1 (Help).
5. Press Enter.

The SETUP SOLVE SSI Primary Menu panel appears.
6. Enter **1** (Add a Region).

The SETUP Specify SOLVE SSI Name panel appears.
7. Enter the name (*ssiname*) and description of the SOLVE Subsystem Interface region you are setting up.

The setup software uses the name to generate the started task JCL. For example, if the name is SOLVESSI, your started task JCL is named SOLVESSI.
8. Complete each of the SETUP panels as they appear. Accept the default values, or specify site-specific values.

Note: Install Utility lets you configure a SOLVE SSI to work with other products, enabling the SSI to be shared.

The Install Utility generates a series of setup jobs into the *dsnpref.NMC1.ssiname.JCL* library.
9. Record the name of the data set into which the JCL was generated in your [post-installation worksheet](#) (see page 175).

Note: If you are setting up a new SSI, continue with these steps. Otherwise, skip the remaining steps in this procedure, verify that the required SSI parameters are present in your existing shared SSI, and update them as necessary.

10. Submit and run the following:

S01SSIAL

Allocates the SOLVE SSI data sets if the value in the Enable the Packet Analyzer field on the SETUP Region Parameters panel is set to YES.

S02SSILD

Copies the PDS members to *dsnpref.NMC1.SSIPARM*.

S03MIGRT

Copies data from earlier releases.

This job is only generated if the value in the Enable the Packet Analyzer field on the SETUP Region Parameters panel is set to YES.

11. Press F3.

The Install Utility Primary Menu panel appears.

Specify the Product Region

The Install Utility lets you set up a region with the products you installed. If you need additional product regions, you can reuse the Install Utility to create them.

Follow these steps:

1. At the ISPF/PDF TSO Command Shell prompt, execute the following command:

```
EXEC 'dsnpref.NMC1.CC2DJCL(INSTALL)'
```

The Install Utility panel appears.

Note: On each of the Install Utility panels, you can use the following keys:

- Enter to proceed to the next panel
- F1 to display online help
- F3 to return to the previous panel
- F4 to exit and return to the main menu

2. Press Enter.

The Install Utility Primary Menu panel appears.

3. Enter **5** (Setup a NetMaster/SOLVE Product Region).

The SETUP Product Region Primary Menu panel appears.

4. Enter **1** (Add a Region).

The SETUP Specify Product Region Name panel appears.

Note: If you want to add this product to an existing region, enter **4** (Add Products and Additional Features to a Region) and select the appropriate region.

5. Enter the name (*rname*) and description of the region you are setting up.

The Install Utility uses the name that you entered to generate local data set names and the started task JCL. For example, if you enter REGION01 as the region name, your started task JCL is REGION01 and a local region file, such as the Virtual File System (VFS), is *dsnpref.REGION01.VFS*.

The SETUP Product Selection panel appears.

6. Enter **S** next to the products you are licensed to include in the region.
7. Complete each of the SETUP panels as they open. Accept the default values, or specify site-specific values.

Note: For information about the fields, press F1 (Help).

Note: On the SETUP Region Information panel, ensure that the value of the Subsystem Interface Identifier matches the value of the SOLVE SSI you intend to use.

The setup software generates a series of setup jobs in the *dsnpref.NMC1.rname.JCL* library.

8. Record the name of the data set into which the JCL was generated in your [post-installation worksheet](#) (see page 175).

9. Submit and run the following jobs in sequence. Do not proceed with any job until the previous job has completed successfully.

S01LCALC

Allocates the region-specific (local) data sets. If you are upgrading and have increased the size of a particular file, modify the JCL to increase the space allocation as required.

S02SHALC

Allocates the shared run-time data sets.

S03LDVIP

Populates the MODS, PANELS, and OSCNTL files.

S04LDVSM

Populates the other VSAM files.

S05LDPDS

Copies some PDS members to *dsnpref.rname*.TESTEXEC or *dsnpref*.PARMLIB for use by the product region. If this product is being added to an existing region, the RUNSYSIN and IIAPARMS are overwritten.

When the region starts for the first time, the values in IIAPARMS set up certain parameter group values. On subsequent startups, the region uses the parameter group values. The IIAPARMS values are then only used if INIRESET=YES is specified or if the VFS data set is reset.

Note: The member names for IIAPARMS and SXPARMS include the domain ID, so they appear as IIAdmid and SXPdmid.

S06MIGRT

Copies site-specific VSAM data from an earlier release.

Note: The utility also generates the following jobs for deploying the configuration files for your region to a target system when a shared DASD is not available: S10DUMP and S11REST. The S10DUMP job creates a backup data set that includes the configuration files for the region, which you deploy to the target system. The S11REST job, when submitted on the target system, restores the configuration files from the backup data set. In addition to deploying the configuration files, also deploy the target libraries. CA MSM can facilitate this deployment.

Note: After your product is installed, it monitors the size of your VSAM data sets. For more information about tuning VSAM data sets, see the *Reference Guide*.

10. Press F3.

The Install Utility Primary Menu panel appears.

Chapter 7: Creating VTAM Definitions and Tables

The topics in this section describe the manual tasks you perform if you are not configuring your product using CA MSM.

You create VTAM definitions and tables to set up your VTAM major node.

This section contains the following topics:

[Create VTAM Definitions and Tables](#) (see page 95)

Create VTAM Definitions and Tables

The Create VTAM Definitions and Tables facility builds the VTAM major node, which contains application definition statements for all ACBs required by your product regions. Perform this task initially when all product regions have been set up. If changes are made to any regions or if additional regions are added later, perform the task again.

Note: You use the major node that you create in this procedure to [activate your VTAM applications](#) (see page 125).

Follow these steps:

1. At the ISPF/PDF TSO Command Shell prompt, execute the following command:

```
EXEC 'dsnpref.NMC1.CC2DJCL(INSTALL)'
```

The Install Utility Primary Menu panel appears.

2. Enter **7** (Create VTAM Definitions and Tables).

The VTAM Primary Menu panel appears.

3. Enter **1** (Create VTAM Definitions and Tables).

The VTAM Data Sets panel appears.

4. Enter the VTAM major node name (*vtamname*) and data set names of the requested IBM data sets.

The VTAM NetMaster/SOLVE ACBs panel appears and displays the prefix for External Interface Package (EIP) ACBs and the names of all product regions and the ACBs associated with them.

Note: If >>> appears, you can use F10 (right) to display all ACBs.

5. Enter the prefix for EIP ACBs.

6. Complete each of the remaining panels as they appear. Accept the default values, or specify site-specific values.

Note: For information about the fields, press F1 (Help).

The Install Utility generates a series of jobs in the *dsnpref*.NMC1.VTAM.JCL library.

7. Record the name of the data set into which the JCL was generated in your [post-installation worksheet](#) (see page 175).
8. Submit and run the following jobs in sequence:

V01LDVTM

Copies major node into SYS1.VTAMLST.

V02ASMOD

Assembles VTAM MODE table.

This job is required only if you want to provide users with access to external applications. Your product uses VTAM mode tables that are assembled and linked into a load library available to VTAM, and the tables lets users access external applications.

Each job should return condition code 0 unless otherwise indicated.

9. Press F3.

The Install Utility Primary Menu panel appears.

10. Enter **X**.

The Install Utility closes.

Note: Press F1 (Help) for information about any panel.

Chapter 8: Preparing the IBM Communications Server

These topics describe how to prepare IBM Communications Server to communicate with this product.

If you do not use IBM Communications Server, skip to [Preparing CA TCPaccess CS](#) (see page 111).

If you use CA TCPaccess Telnet Server as an external Telnet server, continue on to [Preparing CA TCPaccess Telnet Server](#) (see page 109) after you prepared IBM's Communications Server.

This section contains the following topics:

[Review Your SOLVE SSI Configuration](#) (see page 97)

[Set Up the SNMP Agent](#) (see page 98)

[SMF Record Creation](#) (see page 99)

[Define UNIX Authorization for Your Started Task User IDs](#) (see page 101)

[Authorize SOLVE SSI Command Access](#) (see page 101)

[SNA Network Management Interface Setup](#) (see page 102)

[IPSec Network Management Interface Setup](#) (see page 103)

[Authorize Product Region Command Access](#) (see page 106)

[User Authorization to View Packet Payload Data](#) (see page 107)

[User Authorization for IP Security Functions](#) (see page 108)

Review Your SOLVE SSI Configuration

The product region uses the UNIX System Services (USS) shell to issue the NETSTAT (onetstat) command. The interface to the USS shell is provided by a SOLVE SSI connected to your product region and running on the same operating system.

Review the *dsnpref.NMC1.SSIPARM* (SSISYSIN) member, and ensure the following:

- UNIX=YES—To enable the NETSTAT interface
- SMF=YES—To process SMF records

Set Up the SNMP Agent

Note: Do not perform this task if OSNMPD is already configured.

To set up the SNMP agent

1. Configure the SNMP agent (OSNMPD) by following the instructions in the *IBM Communications Server IP Configuration Guide*.
2. Locate the PW.SRC data set in the OSNMPD started task JCL. This data set can be:

- A z/OS data set, for example:

```
//SYSPWSRC DD DISP=SHR,DSN=TCPIP.DATA(PWSRC)
```

- A z/OS UNIX file, for example:

```
/etc/pw.src
```

3. In the PW.SRC data set, configure a community name for use by the local host IP address.

Important! Community names are case sensitive. The default community name is public in lowercase.

For example, with multiple IP addresses, if the Communications Server has the IP addresses 192.168.8.1 and 192.168.1.2, your PW.SRC data set could contain something like the following:

```
public 192.168.0.0 255.255.0.0
```

With a single IP address, if Communications Server has the IP address 192.168.0.1, your PW.SRC data set could contain something like the following:

```
public 192.168.0.1 255.255.255.255
```

It is not necessary to activate the SNMP Query Engine (SNMPQE) because the functions it performs are done internally by your product.

4. Locate the PROFILE data set.
5. Set up the TCP/IP subagent in the PROFILE data set by following the instructions in the *IBM Communications Server IP Configuration Guide*, for example:

```
SACONFIG COMMUNITY public AGENT 161 ENABLED
```

6. Activate the SNMP agent (OSNMPD) by following the instructions in the *IBM Communications Server IP Configuration Guide*.

SMF Record Creation

The Communications Server must be set up to generate the SMF type 119 records for the following:

- Telnet events
- Connection events
- FTP events

The SMF records are intercepted by the SOLVE SSI region and are used by the product region to enable the following:

- Application name generation
- Event history reporting
- Telnet connection identification

The z/OS operating system must also be set up to enable Communications Server SMF record types to be processed.

Generate SMF Records

The configuration members for the Communications Server include parameters that do the following:

- Specify which SMF records are created
- Identify the SMF subtypes

Note: Only SMF record type 119 is intercepted by the SOLVE SSI region.

To ensure SMF records are generated

1. Check the PROFILE.TCPIP configuration member for TCP connect, FTP client, and Telnet client record creation.

The SMFCONFIG statement lets you specify whether or not SMF records are created for the following:

- TCP connection start
- TCP connection end
- FTP and Telnet client records

Example:

```
...  
SMFCONFIG TYPE119 TCPINIT TCPTerm FTPCLIENT TN3270CLIENT  
...
```

An SMF record will not be created if you omit the SMFCONFIG statement or a particular parameter.

2. Check the PROFILE.TCPIP configuration member TELNETPARMS section for Telnet server record creation to ensure that it contains the following line:

```
TELNETPARMS  
...  
; Telnet Server connection SMF logging  
SMFINIT TYPE119  
SMFTERM TYPE119  
ENDTELNETPARMS  
;
```

The SMFINIT statement controls session start and the SMFTERM statement controls session end records.

3. Check the FTP.DATA configuration member to ensure that it contains the following line:

```
SMF TYPE119
```

You should use standard record subtypes and ensure that you set the SMF parameters for FTP to the same type as you set for Telnet, that is, SMF type 119.

The SMF statement may be used to set the default value for all types.

An SMF record will not be created if you omit these parameters.

4. If you have made any changes in step 3, restart the FTP server started task.
5. If you have made any changes in steps 1 or 2, restart the TCP/IP started task.

Note: Alternatively, you can issue these changes in an OBEYFILE.

Define UNIX Authorization for Your Started Task User IDs

The product region requires access to sockets interfaces and therefore requires UNIX System Services authorization provided by an OMVS segment security definition.

For the Packet Analyzer and UNIX functions, the SOLVE SSI region requires UNIX System Services authorization. An OMVS segment security definition provides this authorization.

Set the [UNIX System Services authorization](#) (see page 177) for the following user IDs:

- The started task user ID of the product region
- The started task user ID of SOLVE SSI

Authorize SOLVE SSI Command Access

Note: If you are using CA ACF2 for z/OS, you do not need to perform this task unless it is set up to protect operator commands.

The Packet Analyzer issues VARY TCPIP commands. The user ID associated with your SOLVE SSI region must be authorized by your security system to issue these commands. The OPERCMDS resources to be accessed, and required access levels are as follows:

- MVS.VARY.TCPIP: UPDATE access
- MVS.VARY.TCPIP.PKTTRACE: CONTROL access

Example: Authorization in a CA ACF2 System that Protects Operator Commands

```
$KEY(MVS) TYPE(OPR)
VARY.TCPIP.- UID(uid_string) SERVICE(UPDATE) ALLOW
VARY.TCPIP.PKTTRACE UID(uid_string) SERVICE(DELETE) ALLOW
```

Example: Authorization in a CA Top Secret System

```
TSS PER(XXXXXX) OPERCMD(MVS.VARY.) ACCESS(ALL)
```

Example: Authorization in a RACF System

```
PE MVS.VARY.TCPIP.* CLASS(OPERCMDS) ID(uuuuuuu) ACCESS(UPDATE)
PE MVS.VARY.TCPIP.PKTTRACE CLASS(OPERCMDS) ID(uuuuuuu)
ACCESS(CONTROL)
```

SNA Network Management Interface Setup

The SNA Network Management Interface (SNANMI) of the product requires the VTAM SNAMGMT server to be enabled.

To enable the VTAM SNAMGMT server, specify SNAMGMT=YES in the VTAM start options, VTAMLST member ATCSTRxx.

To enable the SNAMGMT server dynamically, enter the command:

```
F NET,VTAMOPTS,SNAMGMT=YES
```

SNA Network Management Interface Security Requirements

The security requirements for the SNA Network Management Interface are:

- The user ID assigned to the VTAM address space must have an OMVS segment defined and have write access to the /var directory.
- If you use a SERVAUTH class SAF resource to control access to the VTAM SNAMGMT server, the user ID assigned to the SOLVE SSI address space must be permitted access to the resource. The resource name is IST.NETMGMT.*sysname*.SNAMGMT, where *sysname* is the system name where the interface is used.

Access problems to /var and IST.NETMGMT.*sysname*.SNAMGMT are indicated by the presence of messages NSN58n in the SOLVE SSI log.

Examples: Setting IST.NETMGMT.*sysname*.SNAMGMT security

This example sets the security requirements in an CA ACF2 system:

```
SET RESOURCE(SER)
COMPILE
$KEY(IST) TYPE(SER)
  NETMGMT.sysname.SNAMGMT UID(uid) SERVICE(READ) ALLOW
STORE
```

SER

The value set in the CLASMAP definition in the GSO for SERVAUTH resources.

uid

The UID of the region user.

This example sets the security requirements in a CA Top Secret system:

```
TSS PER(userid) SERVAUTH(IST.NETMGMT.sysname.SNAMGMT) ACCESS(READ)
```

userid

The ACID of the region user.

This example sets the security requirements in a RACF system:

```
PER IST.NETMGMT.sysname.SNAMGMT CLASS(SERVAUTH) ID(userid) ACCESS(READ)
```

userid

The user ID of the region.

IPSec Network Management Interface Setup

If you use IPSec, you can use the IPSec Network Management Interface (IPSECNMI) of the product to monitor it. The interface requires the IKED daemon to be active.

IPSec Network Management Interface Security Requirements

The security requirements for the IPSec Network Management Interface are:

- The user ID assigned to the SOLVE SSI address space must have:
 - An OMVS segment defined
 - Permission to enter the /var/sock directory
 - Permission to write to the /var/sock/ipsecmgmt socket
- If you use a SERVAUTH class SAF resource to restrict access to IPSec network management interface, the user ID assigned to the SOLVE SSI address space must be permitted to access to the resources:

`EZB.NETMGMT.sysname.tcpipname.IPSEC.DISPLAY`

`EZB.NETMGMT.sysname.tcpipname.IPSEC.CONTROL`

`EZB.NETMGMT.sysname.sysname.IKED.DISPLAY`

sysname

Specifies the system name where the interface is used.

tcpipname

Specifies the name of the TCP/IP stack.

- If you *don't* use a SERVAUTH class SAF resource to restrict access to IPSec network management interface, the user ID assigned to the SOLVE SSI address space must be *one* of:
 - An OMVS superuser
 - Permitted to access to the FACILITY class SAF resource BPX.SUPERUSER.

Access problems to /var and EZB.NETMGMT.** are indicated by the presence of messages NIS58n in the SOLVE SSI log.

Examples: Setting EZB.NETMGMT.sysname.tcpipname.IPSEC.DISPLAY security

This example sets the security requirements in an CA ACF2 system:

```
SET RESOURCE(SER)  
COMPILE  
$KEY(EZB) TYPE(SER)  
    NETMGMT.sysname.tcpipname.IPSEC.DISPLAY UID(uid) SERVICE(READ) ALLOW  
STORE
```

SER

The value set in the CLASMAP definition in the GSO for SERVAUTH resources.

Uid

The UID of the region user.

This example sets the security requirements in a CA Top Secret system:

```
TSS PER(userid) SERVAUTH(EZB.NETMGMT.sysname.tcpipname.IPSEC.DISPLAY) ACCESS(READ)
```

Userid

The ACID of the region user.

This example sets the security requirements in a RACF system:

```
PER EZB.NETMGMT.sysname.tcpipname.IPSEC.DISPLAY CLASS(SERVAUTH) ID(userid)  
ACCESS(READ)
```

Userid

The user ID of the region.

Authorize Product Region Command Access

Note: If you are using CA ACF2 for z/OS, you do not need to perform this task unless it is set up to protect operator commands.

Your product uses z/OS operator VARY commands to perform some functions. These functions include:

- Packet tracing
- Device activations and deactivations
- Dropping connections
- Verifying Telnet LU status

The user ID associated with your product region must be authorized by your security system to issue these commands. The following OPERCMDS resources require UPDATE access level:

- MVS.VARY.TCPIP.PKTTRACE
- MVS.VARY.TCPIP.OBEYFILE
- MVS.VARY.TCPIP.DROP
- MVS.VARY.TCPIP.TELNET.ACT
- MVS.VARY.TCPIP.TELNET.INACT

Authorize individual users to the OPERCMDS resources if you:

- Plan to configure your system to use SAF user security
- Are using a partial security exit that returns a SAF UTOKEN (for example, NMSAFPX)

Example: Authorization in a CA ACF2 System that Protects Operator Commands

```
$KEY(MVS) TYPE(OPR)
VARY.TCPIP.- UID(uid_string) SERVICE(UPDATE) ALLOW
```

Example: Authorization in a CA Top Secret System

```
TSS PER(XXXXXX) OPERCMD(MVS.VARY.) ACCESS(UPDATE)
```

Example: Authorization in a RACF System

```
PE MVS.VARY.TCPIP.* CLASS(OPERCMDS) ID(uuuuuuu) ACCESS(UPDATE)
```

User Authorization to View Packet Payload Data

Because IP packets can contain sensitive information, authority to view the payload data must be granted by your external security system (CA ACF2 for z/OS, CA Top Secret for z/OS, or RACF). The user must have READ access to NETMSTR.PKTTRACE.*region*, where *region* is the region's ACB name, as specified in the PRI= parameter in the RUNSYSIN member.

CA Top Secret

To set up definitions to allow access to SmartTrace in your region with ACB NMTEST, issue the following commands:

```
TSS ADD(dept) IBMFAC(NETMSTR)
TSS PERMIT(USER1) IBMFAC(NETMSTR.PKTTRACE.*) ACCESS(NONE)
```

To allow user USER1 to access SmartTrace data, issue the following command:

```
TSS PERMIT(USER1) IBMFAC(NETMSTR.PKTTRACE.NMTEST) ACCESS(CONTROL)
```

CA ACF2

To set up definitions to allow access to SmartTrace in your region with ACB NMTEST, issue the following commands:

```
[ACF]
SET RESOURCE(FAC)
COMPILE *
$KEY(NETMSTR.PKTTRACE.*) TYPE(FAC)
```

To allow user USER1 to access SmartTrace data, issue the following command:

```
$KEY(NETMSTR.PKTTRACE.NMTEST) TYPE(FAC) USER1(USER1) READ(ALLOW)
STORE
[END]
```

RACF

To set up definitions to allow access to SmartTrace in your region with ACB NMTEST, issue the following commands:

```
RDEFINE FACILITY NETMSTR.PKTTRACE.* UACC(NONE)
RDEFINE FACILITY NETMSTR.PKTTRACE.NMTEST UACC(NONE)
SETROPTS RACLIST(FACILITY) REFRESH
```

To allow user USER1 to access SmartTrace data, issue the following command:

```
PERMIT NETMSTR.PKTTRACE.NMTEST CLASS(FACILITY) ID(USER1) ACCESS(READ)
```

User Authorization for IP Security Functions

If you use IPsec, your security system must authorize the individual users for read access to the SERVAUTH resource:

- To view data about IP security:
`EZB.IPSECCMD.sysname.stackname.DISPLAY`
- To perform a control function against a tunnel:
`EZB.IPSECCMD.sysname.stackname.CONTROL`

Examples: Authorizing IP security displays and commands

This example authorizes IP security on a CA ACF2 system:

```
$KEY(MVS) TYPE(OPR) EZB.IPSECCMD.sysname.stackname- UID(uid_string) SERVICE(READ)
ALLOW
```

This example authorizes IP security on a CA Top Secret System:

```
TSS PER(acid) OPERCMD(EZB.IPSECCMD.sysname.stackname) ACCESS(READ)
```

This example authorizes IP security on a RACF System:

```
PE EZB.IPSECCMD.sysname.stackname CLASS(SERVAUTH) ID(uuuuuuu) ACCESS(READ)
```

Chapter 9: Preparing CA TCPaccess Telnet Server

If you use CA TCPaccess Telnet Server r6.2 (for example, as an external Telnet server for IBM's Communications Server), you need to prepare it to communicate with your product.

This section contains the following topics:

[Enable Event Interface](#) (see page 109)

[Restart CA TCPaccess](#) (see page 110)

Enable Event Interface

You must set up the server to do the following:

- Have NMDSPAXS defined as an exit
- Generate the required SMF records

This setup ensures that the server provides the data that is required by your product. The data is intercepted by the SOLVE SSI region and used by the product region to enable the following:

- Application name generation
- Event history reporting

Define the Server Exit

You first need to define the server exit.

To define the server exit

1. Open the IJTCFGxx configuration member.
2. Define NMDSPAXS as an exit by adding the following statement to the IJTCFGxx member:

`EXIT PROGRAM (NMDSPAXS)`
3. Insert the NMDSPAXS definition in the first position of the exit list. This ensures that the exit is always called.
4. Copy the NMDSPAXS load module supplied in *dsnpref.NMC1.CC2DLOAD* to an accessible library, for example, a library in the server started task STEPLIB.

Generate SMF Records

After you define the exit, you need to generate SMF records.

To set up the server to generate SMF records

1. Access the IJTFCGxx configuration member. This is where the SMF record type and sub-types are specified.
2. Check that all of the subtypes that you require will be generated.

The SMF statement SUBTYPE parameter allows specific subtypes to be selected or suppressed. To generate subtypes:

- If your SMF statement does not specify SUBTYPE, leave it as it is
- If the parameter is set to ALL, leave it as it is
- If the parameter is set to NONE, set it to ALL or a list of the subtypes that you require
- If the parameter is set to a list of subtypes, set it to ALL or a list of the subtypes that you require. The following subtype is used by your product: SUBTYPE 24—Telnet server session termination.

Restart CA TCPaccess

If you have made changes to your IJTFCGxx configuration member, you need to restart the server.

To restart the server

1. Restart the server to bring the changes into effect.
2. Check the job log and the SYSLOG for the presence of the following messages:

```
T00EX004I NMDSPAXS: N6XA01 Activity log message interface initialized
T00EX004I NMDSPAXS: N6XA02 Receiver ID $IPXssid will monitor messages from
TCPaccess
T00EX004I NMDSPAXS: N6XA03 NetMaster AXS exit EP:exit_entry_point
Compiled:compilation_timestamp

ssid is the SSID of the server job.
```

These messages are logged during initialization. Their presence indicates that the interface has been set up correctly.

Chapter 10: Preparing CA TCPaccess CS

This chapter describes how to prepare CA TCPaccess CS to communicate with your product.

If you do not use CA TCPaccess CS, skip to the next chapter.

This section contains the following topics:

[Enable Event Interface](#) (see page 111)

[Set Up DNR Members](#) (see page 113)

[Enable Access to SNMP Data](#) (see page 113)

[Restart CA TCPaccess](#) (see page 114)

[User Authorization to View Packet Payload Data](#) (see page 114)

Enable Event Interface

You must set up the server to do the following:

- Have NMDSPAXS defined as an exit
- Generate the required SMF records

This setup ensures that the server provides the data that is required by your product. The data is intercepted by the SOLVE SSI region and used by the product region to enable the following:

- Application name generation
- Event history reporting

Define the Server Exit

You first need to define the server exit.

To define the server exit

1. Open the IJTFCGxx configuration member.
2. Define NMDSPAXS as an exit by adding the following statement to the IJTFCGxx member:

`EXIT PROGRAM (NMDSPAXS)`
3. Insert the NMDSPAXS definition in the first position of the exit list. This ensures that the exit is always called.
4. Copy the NMDSPAXS load module supplied in *dsnpref.NMC1.CC2DLOAD* to an accessible library, for example, a library in the server started task STEPLIB.

Generate SMF Records

After you define the exit, you need to generate SMF records.

To set up the server to generate SMF records

1. Access the IJTFCGxx configuration member. This is where the SMF record type and sub-types are specified.
2. Check that all of the subtypes that you require will be generated.

The SMF statement SUBTYPE parameter allows specific subtypes to be selected or suppressed. To generate subtypes:

- If your SMF statement does not specify SUBTYPE, leave it as it is
- If the parameter is set to ALL, leave it as it is
- If the parameter is set to NONE, set it to ALL or a list of the subtypes that you require
- If the parameter is set to a list of subtypes, set it to ALL or a list of the subtypes that you require. The following subtypes are used by your product:
 - SUBTYPE 20—FTP data set transfer completion (RETR, STOR, and APPE)
 - SUBTYPE 21—FTP data set modification (REN and DELE)
 - SUBTYPE 23—Telnet server session termination
 - SUBTYPE 113—TCP close

Set Up DNR Members

You must ensure that your CA TCPaccess CS Domain Name Resolver (DNR) members can translate the CA TCPaccess CS subsystem name into an IP address and a fully-qualified host name.

To set up DNR members

1. Enable translation from subsystem name to fully-qualified domain name.
For example, if your CA TCPaccess CS subsystem name is ACSS and its fully-qualified domain name is MVS.SITE1.COM, enter a line like the following into your DNRALCxx member:

```
ACSS MVS.SITE1.COM.
```

Specify the domain name (rather than an IP address) and end it with a period (.).

2. Enable local translation of the fully qualified host name to an IP address.
For example, if the IP address of MVS.SITE1.COM. is 172.24.123.112, enter a line like the following into your DNRHSTxx member:

```
MVS.SITE1.COM. 172.24.123.112
```

3. Ensure that the HOSTTABLE statement in the DNRCFGxx member points to the correct DNRHSTxx member.
4. Restart DNR. You do not need to restart CA TCPaccess CS to introduce changes to the DNR tables. For example:

```
F stackname,STOP DNR TASK(n)
F stackname,START DNR CNFG(xx)
```

TASK(n) is the DNR task number used by the site.

Enable Access to SNMP Data

Your product accesses information about CA TCPaccess CS by using SNMP.

To enable these functions, you must activate the SNMP Agent by updating the SNMCFGxx member in the CA TCPaccess CS PARM data set. Make sure that you have a community value statement, which includes the community name. The default community name is *public* in lower case. You do not need to restart CA TCPaccess CS.

To activate SNMP, issue **/F stackname,START SNM CNFG(xx)**.

Make sure you update the STARTxx member to include the following:

```
'START SNM CNFG(xx)
```

Restart CA TCPaccess

If you have made changes to your IJTCFGxx configuration member, you need to restart the server.

To restart the server

1. Restart the server to bring the changes into effect.
2. Check the job log and the SYSLOG for the presence of the following messages:

```
T00EX004I NMDSPAXS: N6XA01 Activity log message interface initialized
T00EX004I NMDSPAXS: N6XA02 Receiver ID $IPXssid will monitor messages from
TCPaccess
```

```
T00EX004I NMDSPAXS: N6XA03 NetMaster AXS exit EP:exit_entry_point
Compiled:compilation_timestamp
```

ssid is the SSID of the server job.

These messages are logged during initialization. Their presence indicates that the interface has been set up correctly.

User Authorization to View Packet Payload Data

Because IP packets can contain sensitive information, authority to view the payload data must be granted by your external security system (CA ACF2 for z/OS, CA Top Secret for z/OS, or RACF). The user must have READ access to NETMSTR.PKTTRACE.*region*, where *region* is the region's ACB name, as specified in the PRI= parameter in the RUNSYSIN member.

CA Top Secret

To set up definitions to allow access to SmartTrace in your region with ACB NMTEST, issue the following commands:

```
TSS ADD(dept) IBMFAC(NETMSTR)
TSS PERMIT(USER1) IBMFAC(NETMSTR.PKTTRACE.*) ACCESS(NONE)
```

To allow user USER1 to access SmartTrace data, issue the following command:

```
TSS PERMIT(USER1) IBMFAC(NETMSTR.PKTTRACE.NMTEST) ACCESS(CONTROL)
```

CA ACF2

To set up definitions to allow access to SmartTrace in your region with ACB NMTEST, issue the following commands:

```
[ACF]
SET RESOURCE(FAC)
COMPILE *
$KEY(NETMSTR.PKTTRACE.*) TYPE(FAC)
```

To allow user USER1 to access SmartTrace data, issue the following command:

```
$KEY(NETMSTR.PKTTRACE.NMTEST) TYPE(FAC) USER1(USER1) READ(ALLOW)
STORE
[END]
```

RACF

To set up definitions to allow access to SmartTrace in your region with ACB NMTEST, issue the following commands:

```
RDEFINE FACILITY NETMSTR.PKTTRACE.* UACC(NONE)
RDEFINE FACILITY NETMSTR.PKTTRACE.NMTEST UACC(NONE)
SETROPTS RACLIST(FACILITY) REFRESH
```

To allow user USER1 to access SmartTrace data, issue the following command:

```
PERMIT NETMSTR.PKTTRACE.NMTEST CLASS(FACILITY) ID(USER1) ACCESS(READ)
```


Chapter 11: Preparing to Start Your Product

Before CA NetMaster NM for TCP/IP can be started and used, preparation tasks are required.

This section contains the following topics:

[Started Task JCL Setup](#) (see page 117)

[Operational Considerations](#) (see page 123)

[Subsystem Identifier Setup](#) (see page 123)

[Load Libraries](#) (see page 123)

[Assign Consoles](#) (see page 124)

[Activate VTAM Applications](#) (see page 125)

[Enable Auditing by CA Auditor](#) (see page 125)

The Install Utility places RUNSYSIN (for the product region) in a default data set. If you move this member to a more secure data set, you must update the started task JCL to point to the new data set.

Started Task JCL Setup

The Install Utility places the following SYSIN and parameter members into default data sets:

- SSIPARMS and SSISYSIN—for SOLVE SSI
- RUNSYSIN—for the product region

If you move these members into a more secure data set, update the started task JCL and SYSIN members to point to the new data set.

TESTEXEC Data Set

The install utility populates the TESTEXEC data set based on the values entered during the installation and setup process.

Review the members in TESTEXEC to:

- Ensure that they meet your site-specific requirements
- Reapply any previous customization that is still required

Review the following members in *dsnpref.rname*.TESTEXEC:

NMREADY

Is the NCL procedure that is executed as part of system initialization after the VTAM ACBs have been opened successfully.

NMINIT

Is the NCL procedure that is executed as part of system initialization before the VTAM ACBs are opened.

Do not:

- Code any SYSPARMS commands in the NMINIT or NMREADY procedures.
- Activate or modify links, or use commands such as DEFLINK, DEFTRANS, and ISR in NMINIT or NMREADY. In a multisystem network, the region uses link definitions during initialization. Defining DEFLINK, DEFTRANS, and ISR in these procedures can interfere with region linkage.

Started Task Product Region Parameter Member

The Install Utility generates the RUNSYSIN member using the values that are entered during the installation and setup process.

RUNSYSIN specifies the product region parameters.

Review RUNSYSIN to:

- Ensure that it meets your site-specific requirements
- Reapply any previous customization that is still required

If you have set SUBS=YES in the member, you can update the RUNSYSIN started task members to use z/OS static system symbols. System symbols assist in the planning of future deployment.

Review the following parameters in *dsnpref.rname*.TESTEXEC(RUNSYSIN):

PPREF='XOPT=SDUMP'

Specifies that ABEND dumps are written to the SYS1.DUMP data set.

If you do not want SYS1.DUMP data sets for dumps, remove the parameter and add the SYSMDUMP DD statement to the generated task in *dsnpref.NMC1.rname*.JCL(*rname*).

PPREF='INIFILE=??????'

Specifies the INI file that is used for parameter customizations.

To use a migrated INI file, uncomment the parameter and replace the question marks with the name of the INI file.

SOLVE SSI Started Task Parameter Member

The Install Utility generates the SSIPARM data set based on the values entered during the installation and setup process.

SSIPARM specifies the SOLVE SSI started task parameters.

Review the data set to:

- Ensure that the members meet your site-specific requirements
- Reapply any previous customization that is still required

Review the following members in *dsnpref.NMC1.SSIPARM*:

SSISYSIN

(Optional) (If you are using an existing shared SOLVE SSI region, you do not have to review this member.)

If SUBS=YES is set, you can update the SSISYSIN started task member to use z/OS static system symbols. System symbols assist in the planning of future deployment.

SSIPARMS

(Optional) (If you are using an existing shared SOLVE SSI region, you do not have to review this member.)

This member is present only if you created it when you specified the SOLVE SSI region.

Parameters can be shared with any other products using this SOLVE SSI. Review these parameters, and ensure that they are set correctly for the products (these parameters can be in SSISYSIN or SSIPARMS).

Note: For more information about sharing a SOLVE SSI, see the *SOLVE Subsystem Interface Guide*.

Review and Copy the SOLVE SSI Started Task

The Install Utility generates a SOLVE SSI started task that you must review to ensure that it meets your site-specific requirements; if necessary, reapply any previous customization that is still required.

Note: If you are using an existing shared SOLVE SSI region, skip this procedure.

Use this procedure to review, update, and copy the SOLVE SSI started task to a procedure library.

Note: To assist you in the planning of future deployment, you can update the SOLVE SSI started task to use z/OS static system symbols.

Follow these steps:

1. Review and update the DD statements in the SOLVE SSI started task member *dsnpref.NMC1.ssiname.JCL(ssiname)* for your site-specific requirements.
2. Copy the reviewed member to SYSx.PROCLIB.

Set Up OSA/SF Support

If you run OSA/SF on the system, your product region can use it to monitor the OSAs. To enable OSA/SF functionality, the OSA/SF load library must be available to your product region.

The OSA/SF API task is used to:

- Monitor OSA performance
- Obtain configuration information for OSA resources

To set up OSA/SF support

1. Examine the z/OS link list for SYS1.SIOALMOD. If SYS1.SIOALMOD is not in the link list, add it to the STEPLIB DD statement in the product region started task member *dsnpref.NMC1.rname.JCL(rname)*. For example:

```
//STEPLIB DD DSN=dsnpref.NMC1.CC2DLOAD,DISP=SHR
//          DD DSN=dsnpref.NMC1.CC2DPLD,DISP=SHR
//          DD DSN=SYS1.SIOALMOD,DISP=SHR
```

2. Ensure that the following are in the same LPAR:
 - The TCP/IP stack with the primary OSA device definition
 - OSA/SF
 - Your product region

For more information about defining resources to monitor OSAs, see the *Administration Guide*.

Review and Copy the Product Region Started Task

The Install Utility generates a product region started task that you must review to ensure that it meets your site-specific requirements; if necessary, reapply any previous customization that is still required.

Use this procedure to review, update, and copy the started task to a procedure library.

Note: To assist you in the planning of future deployment, you can update the product region started task to use z/OS static system symbols.

Follow these steps:

1. Review and update the DD statements in the product region started task member *dsnpref.NMC1.rname.JCL(rname)* for your site-specific requirements.
2. Copy the reviewed member to SYSx.PROCLIB.

Enable the NETSTAT Interface

Note: This topic only applies if you are using CA TCPaccess CS.

To enable the NETSTAT interface, access the CA TCPaccess CS LINK library. Determine if the CA TCPaccess CS LINK library is included in the LINKLIST. If not, add the CA TCPaccess CS LINK library to the STEPLIB concatenation in *dsnpref.NMC1.rname.JCL(rname)*.

For more information, see the *CA TCPaccess Communication Server System Management Guide*.

Operational Considerations

The Packet Analyzer intercepts real time data from TCP/IP stacks, so it is important that the SOLVE SSI runs with sufficient system resources allocated. Review your workload manager definitions to ensure they reflect this requirement and change accordingly.

You should also start the SOLVE SSI as early as possible in the IPL process, immediately after any TCP/IP stack and before the CA NetMaster NM for TCP/IP region, to ensure the statistics reported by the Packet Analyzer are complete.

Subsystem Identifier Setup

The setup of your product environment usually requires the following subsystem identifier (SSID) values that were defined during the [setup process](#) (see page 89):

- An SSID value for the subsystem identifier for the SOLVE SSI—The SOLVE SSI started task automatically identifies this SSID value to the system.
- An SSID value to enable the use of z/OS commands and messages—This SSID is named the AOM subsystem interface ID (AOM SSID). The product region started task automatically identifies this SSID value to the system.

If you want the SSID values to be set permanently and available at system IPL time, you can set them in the SYS1.PARMLIB(IEFSSNxx) member. If you use this member, ensure that you add the AOM SSID for the region first (after JES) in the list of subsystem names, because the first region listed in the SYS1.PARMLIB(IEFSSNxx) member controls the processing of messages by the subsystem interface.

Load Libraries

Most products have their own load library but also require the load libraries of supporting services. The following load libraries must be APF-authorized:

- CC2DLOAD

- CC2DPLD (If SSL is installed)

Authorization of the Load Libraries

To APF-authorize your load libraries, add the run-time load libraries to the SYS1.PARMLIB(IEAAPFxx) APF list.

To dynamically APF-authorize the load libraries, issue the following z/OS command:

```
SETPROG APF,ADD,DSNAME=?loadLib,VOLUME=?volser
```

?loadlib

Specifies the name of the load library.

?volser

Specifies its volume serial number.

To dynamically APF-authorize load libraries controlled by SMS, issue the following z/OS command:

```
SETPROG APF,ADD,DSNAME=?loadLib,SMS
```

Assign Consoles

Your product needs a pool of consoles (either JES or extended MCS consoles) to issue system commands. As delivered, this product uses extended MCS consoles that are dynamically defined.

To use JES consoles instead of the default MCS consoles, define at least six consoles that are *not* used by other products.

Follow these steps:

1. Open the SYS1.PARMLIB(CONSOLxx) member.
2. Add the following statement for each console you want to define:

```
CONSOLE DEVNUM(SUBSYSTEM)...
```

An IPL is required to activate the updated CONSOLxx member. To start using JES consoles, you must also update the \$RM CONSOLES [Customizer parameter group](#) (see page 135).

Activate VTAM Applications

You must activate VTAM applications for your regions. The Create VTAM Definitions and Tables facility builds a VTAM major node that contains APPL definitions for all product regions. The member V01LDVTM copies *vtamname* to SYS1.VTAMLST, which is the VTAM library that contains all the major node and application definitions used by your product.

Follow these steps:

1. Add *vtamname* to the startup list in SYS1.VTAMLST(ATCCONxx).
2. Activate the VTAM major node by entering the following VTAM command:

`V NET,ACT,ID=vtamname`
3. Check that all of the applications are defined to VTAM after the activation. To do this, display the major node by entering the following VTAM command:

`D NET,ID=vtamname,E`

Enable Auditing by CA Auditor

If your auditors require CA Auditor or CA Common Inventory Service to know of this product running on your system, put a load module in your system LNKLST.

To define the load module to the system LNKLST, include the library *dsnpref*.NMC1.CC2DLINK in the system LNKLST SYS1.PARMLIB(PROGxx), for example:

`LNKLST ADD NAME(LNKLST00) DSNAME(dsnpref.NMC1.CC2DLINK)`

Note: Common load modules are used for all CA Mainframe Network Management products. You only need to include one copy of this *dsnpref*.NMC1.CC2DLINK library in the system LNKLST.

Chapter 12: Performing Initial Migration

When you specify your regions, the Install Utility migrates some of your data from the earlier release. You perform some additional migration tasks before you start your product region.

This section contains the following topics:

[NPF and SAF Security Members](#) (see page 127)

More information:

[Migration Preparation](#) (see page 20)

NPF and SAF Security Members

The Install Utility generates Network Partitioning Facility (NPF) and System Authorization Facility (SAF) security members. If you have previously customized any of these security members, update the regenerated members with your changes.

Chapter 13: Starting Up

This section contains the following topics:

[Start the SOLVE SSI Region](#) (see page 129)

[Restart the SOLVE SSI Region](#) (see page 130)

[Start the Product Region](#) (see page 130)

[Perform the Initial Logon](#) (see page 131)

[Add the Initial Administrator User ID](#) (see page 131)

[Perform Subsequent Logon](#) (see page 132)

Note: If you want to run other products in the CA Mainframe Network Management family in this region, before proceeding, complete the tasks described in the *Installation Guide* for the other products.

Start the SOLVE SSI Region

You perform this procedure only if you use a new SOLVE SSI region.

Notes:

- If you are using an existing shared SOLVE SSI region and did not make any changes when [specifying the SOLVE SSI region](#) (see page 90), skip this procedure.
- If you are using an existing shared SOLVE SSI region and have made changes, skip this procedure and proceed to [restarting the SOLVE SSI region](#) (see page 130).

To start the SOLVE SSI region, issue the following command from the MVS console:

```
S ssiname,REUSASID=YES
```

ssiname is the name you specified for the SOLVE SSI during the setup process.

Note: If you use cross memory services but do *not* specify REUSASID=YES, and SOLVE SSI terminates, the address space ID is not available until after the next IPL.

To stop the SOLVE SSI started task, issue the following command from the MVS console:

```
P ssiname
```

Restart the SOLVE SSI Region

You perform this procedure only if you are using an existing shared SOLVE SSI region and made changes when [specifying the SOLVE SSI region](#) (see page 90).

Follow these steps:

1. Stop the SOLVE SSI started task, issue the following command from the MVS console:

`P ssiname`
2. Start the SOLVE SSI region, issue the following command from the MVS console:

`S ssiname,REUSASID=YES`

Note: If you use cross memory services but do *not* specify REUSASID=YES, and SOLVE SSI terminates, the address space ID is not available until after the next IPL.

Start the Product Region

To start the product region, issue the following command:

```
S rname,REUSASID=YES
```

rname is the name you specified for the region during the setup process.

Note: If you use cross memory services but do *not* specify REUSASID=YES, and the region terminates, the address space ID is not available until after the next IPL.

Note: To stop the started task, issue the following command from the MVS console:
`P rname.`

Perform the Initial Logon

Note: If your region is using an existing UAMS data set, you will already have an administrator user ID available for the region. You can use that ID to log on to the region.

Follow these steps:

1. Log on to the product region. You can use the VTAM logon command:

```
LOGON APPLID(priacbnm)
```

priacbnm is the name of the primary VTAM ACB application nominated in the *PPREF='PRI=priacbnm'* command in *dsnpref.rname.TESTEXEC(RUNSYSIN)*.

The region logon panel appears.

2. Enter the user ID **INSTALL** and password **99999999**, and press Enter.

The UAMS : Primary Menu appears.

The INSTALL 99999999 is a special user ID and password combination that can be used once only, and is accepted if the USERID data set is empty. The only functions that the INSTALL user ID can perform are those associated with user ID maintenance.

Add the Initial Administrator User ID

The only functions that the INSTALL user ID can perform are those functions associated with user ID maintenance. Therefore, you must add an initial administrator user ID.

Note: If you are using a full security exit, user authorities are not specified through UAMS. Specify these authorities as structured fields in your security exit. For more information, see the *Security Guide*.

To define an initial user with full authority to UAMS

1. At the UAMS : Primary Menu, type the initial administrator user ID in the User field, **USER** in the Definition Type field, and select the **A – Add User Definition** option.

The UAMS : User Details panel appears.

2. Type the initial password and user details for this initial user ID.

Important! The user must change the password again at first logon.

3. Go to the UAMS definition panels and ensure that you give full authority to this initial user to perform future administration tasks. Set the following minimum values:

User Authorities panel, page 2

Authority Level: 255

APPC Access Key: ALL

APPC Access Lock: ALL

Access Authorities panel, page 3

Set all fields to Y.

Network Management Details panel, page 7

Set fields that correspond to the features your site has configured to Y or the maximum authority.

AOM General Details panel, page 10

AOM Message receipt: Y

AOM MVS Details panel, page 11

Console Authority: M

Print Services Manager Details panel, page 12

For all fields, set the maximum authority (1 through 4).

Report Writer Details panel, page 13

For all fields, set the maximum authority (1 through 4).

4. Press F3.

The user definition is saved.

Perform Subsequent Logon

You are now ready to log on to your product and begin using it as an authorized user.

Follow these steps:

1. Press F3 to log off the product region.
2. Log on using your new initial administrator user ID and password.
3. If necessary, change your password by typing **U.P**, confirm your change, and press F3 (File) to save the change.

Notes:

- If you set SEC=PARTSAF or SEC=NMSAF in the RUNSYSIN member, you are not required to change your password.
- (Optional) To enable users to logon to the product from TSO, add the:
 - *dsprefix.NMC1.CC2DLMD0* data set to LNKST or STEPLIB concatenation for the appropriate TSO procedure
 - *dsprefix.NMC1.CC2DSAMP* data set to the SYSHELP concatenation for the appropriate TSO procedure

Chapter 14: Customizing Your Product

Note: After completing customization, you can use product system variables and z/OS static system symbols to help you plan future deployment to multiple regions. You generate an initialization (INI) file where you can use these variables and symbols. For information about setting up the INI file, see the *Administration Guide*.

This section contains the following topics:

[Initial Customization Requirements](#) (see page 135)

[Web Browser Settings](#) (see page 140)

[Additional Parameter Groups](#) (see page 141)

[Discover System Resources](#) (see page 142)

[Set Up the System Image to Load on Restart](#) (see page 144)

[Initialization Failures](#) (see page 145)

[Review Region Status](#) (see page 147)

[Perform Additional Customization](#) (see page 147)

Initial Customization Requirements

You must set various parameters for your site-specific requirements. Use Customizer to review and update the parameter groups in your product region.

Note: Customizer is used to set the majority of your region parameters. If you need to permanently change any SYSPARMS values that are not handled by Customizer, [contact Technical Support](#) (see page 4).

Important! Setting certain SYSPARMS to values other than the defaults can render certain product features inoperable.

Customization can only be performed by a user with [UAMS maintenance authority](#) (see page 131). That user's UAMS definition should have an APPC Access Key and Lock value of ALL.

Customizer Setup Types

From the Customizer : System Parameters panel, you can select the following options:

Fast Setup

Customizes the required parameter groups and quickly implements your region. It provides default values wherever possible, but lets you review all the required parameter groups to ensure that they match your installation standards. You can customize other parameters at a later time.

Note: You must review all the parameter groups in this option for the region to become operational.

Custom Setup

Customizes the required parameter groups and additional file and data set names, to bring the system operation closer to your installation standards. This option quickly implements your region and still lets you perform some extra customization. It provides some default values, lets you specify names for certain files and data sets, and lets you review the required parameter groups (which are highlighted).

Complete Setup

Customizes all initialization and customization parameters.

Customize Parameter Values

You can use the provided default values or customize the parameter values to suit the requirements of your site.

Note: All parameters have default values.

Follow these steps:

1. Enter **U** next to the parameter group that you want to review, and make the necessary changes for your site.
2. Press F6 (Action) to apply the change immediately. You can view the results by pressing F5 (ILog).

Note: The F6 option is not available for some parameters.

3. Press F3 (File) to save your changes and indicate that you have reviewed the group.

The value you assign to a parameter is associated with one or more actions, such as setting SYSPARMS or allocating data sets. You can action some parameter groups as soon as you enter appropriate values on the parameter panel. However, when you change the value of some parameters, for example, MODS file names, these parameter values can only be applied by restarting the product region.

Note: If you change a parameter, perform an action, and then cancel that action, the new value will be in effect for that action; but when you restart, the value will return to the last saved value. In addition, you can change a value and save it without applying it to have it take effect on the next startup.

Interrupted Customization

If you exit the customization process before reviewing all required parameter groups, you are presented with a confirmation panel. You can log off and continue with the customization later. Alternatively, another authorized user can log on and complete the customization process. Users cannot access the region until all the required parameter groups have been reviewed.

Update and Review the Fast Setup Customization Parameters

To begin the process of updating and reviewing the Fast Setup Customization parameters, select the Fast Setup Customization Parameters option. The Customizer : Fast Setup panel appears.

Implement System Identification Parameters

Use this procedure to implement system identification parameters.

Follow these steps:

1. Enter **U** next to the System Identifications parameter group.
The SYSTEMID - System Identifications panel appears. The parameter group has two panels.
2. Complete the fields on the panels. For information about the fields, press F1 (Help).
3. Press F6 (Action) to action the entries.
4. Press F3 (File) to save your settings.
The Customizer : Fast Setup panel appears with the Reviewed column marked Yes for the parameter group.

Note: The system ID does not take effect until the next system initialization.

Implement Operating System Identifiers Parameters

Use this procedure to implement the operating system identifiers.

Follow these steps:

1. Enter **U** next to the Operating System Identifiers parameter group.
The OPSYSIDS - Operating System Identifiers panel appears.
Complete the fields on this panel. If the system uses the JES3 job entry subsystem, ensure that information about the job entry subsystem is updated.
Note: Press F1 (Help) for more information.
2. Press F6 (Action) to action the entries.
3. Press F3 (File) to save your settings.
The Customizer : Fast Setup panel appears with the Reviewed column marked Yes for the parameter group.

Implement the TCP/IP Sockets Interface Parameters

Use this procedure to enable TCP/IP support.

Access to sockets interfaces requires [UNIX System Services authorization](#) (see page 177) provided by an OMVS segment security definition.

To implement the TCP/IP sockets interface parameters

1. Enter **U** next to the TCP/IP Sockets Interface parameter group.
The first SOCKETS - TCP/IP Sockets Interface panel appears.
2. Tab to the TCP/IP Software Type input field, and enter the required value.
Only one type of TCP/IP software can be configured as the sockets interface in each region.
3. Complete the remaining fields on the first panel.
Note: For more information, press F1 (Help).
The Inbound Connections Port field contains a default port number. If another region on this system is already using that number, tab to the field and change it.
Important! The port number must be unique on a system.
4. Press F8.
The second panel for this parameter group appears.
5. Complete the fields on the panel.
Specify the details of the TCP/IP software as follows:
 - If you are using the IBM Communications Server, enter your TCPIP.DATA data set name in the TCPIP.DATA DSN field and review the Domain Name Resolution fields.
 - If you are using CA TCPaccess CS, tab to the CA TCPaccess CS SSID field and enter the required SSID. If you are unsure of the CA TCPaccess CS subsystem ID, access the CA TCPaccess CS startup procedure and check the value of the SSN parameter.
6. Press F6 (Action) to set the specified values and start the interface.
7. Press F3 (File) to save your settings.
The Customizer : Complete Setup panel appears with the TCP/IP Sockets Interface Reviewed field marked as YES.
8. Press F3 (Exit).
The Customizer : System Parameters panel appears.

Implement the WebCenter Parameters

Use this procedure to implement access to the WebCenter interface.

To implement the WebCenter parameters

1. Enter **U** next to the WebCenter Web Interface parameter group.
The WEBCENTER - WebCenter Web Interface panel appears.
2. Tab to the Web Interface Port input field, and enter a unique value.
3. Complete the fields on the panel.
Note: For more information, press F1 (Help).
4. To use SSL to encrypt WebCenter traffic, press F11.
The panel that sets SSL parameters appears.
5. When you have completed all the fields, press F6 (Action) to set the specified values.
If you specified a WebCenter port number, note the generated WebCenter Access URL because you use this URL to access your product region using WebCenter.
6. Press F3 (File) to save your settings.
The Customizer : Fast Setup panel appears with the Reviewed column marked Yes for the WebCenter web interface parameters.
7. Press F3 (Exit).
You are returned to the Customizer : System Parameters panel, and the WebCenter parameters are implemented.

Web Browser Settings

If you are using WebCenter, instruct all users to take the following actions:

- Clear the cache of their web browser to prevent them from getting a mix of old and new web files.
- Disable pop-up blocker, or define WebCenter as an allowed website.

Additional Parameter Groups

Depending on which product features you want to implement, you may want to review other parameter groups and add any values that you saved from your old product region.

You can review these parameter groups now or later, as follows:

- **Now**—Select the Complete Setup Customization Parameters option to list all parameter groups and review the relevant groups. When you complete the review, exit the list and the Customizer : System Parameters panel.
- **Later**—Exit the Customizer : System Parameters panel. (When you are ready to review these parameter groups, enter **/PARMS** to list the groups.)

Enable Metrics Feed to CA APM

Perform this task only if you have a CA Cross-Enterprise APM license and you want to feed data to CA APM from this product region.

The APMEPAGENT parameter group configures the metrics feed to CA APM.

Note: For information about how to configure CA APM for the integration, see *CA Cross-Enterprise Application Performance Management Integration Guide*.

Follow these steps:

1. Enter **U** next to the APMEPAGENT parameter group.
The APMEPAGENT - CA Introscope EPAgent panel appears.
2. Complete the fields as required:
 - Set the Enable EPAgent Client? field to **YES**.
 - Set the IP Addr/Host Name to identify your CA Introscope Environment Performance Agent.

Note: For information about the fields, press F1 (Help).

3. Press F6 (Action) to action the entries.
The region starts to feed metrics.
4. Press F3 (File) to save your settings.
The Customizer : Complete Setup panel appears.

Implement External Applications Access

Note: You only need to perform this task if you have installed CA NetSpy and you want the NetSpy option to appear on the primary menu of your product region.

To implement external application access

1. Enter **U** beside the \$RM EXTAPPLS parameter group.
The EXTAPPLS - External Applications Access panel appears.
2. Under NetSpy Application Specifications, enter the NetSpy ACB Name. For information about the remaining fields, press F1 (Help).
3. Press F6 (Action) to action the entries.
4. Press F3 (File) to save your settings.
The Customizer : Complete Setup panel appears.

Implement Links to CA NetSpy Network Performance

Note: Perform this task only if you have installed CA NetSpy and you want its data to be available to your product region.

Follow these steps:

1. Enter **U** beside the \$ES NETSPYLINKS parameter group.
The NETSPYLINKS - Links to NetSpy Applications panel appears.
2. Enter the CA NetSpy X-communication (NSYXNAME) ACB name. This name is used for the following communications:
 - NetSpy-to-NetSpy communication
 - NetSpy-to-NetMaster communication

Note: For information about the fields, press F1 (Help).
3. Press F6 (Action) to action the entries.
4. Press F3 (File) to save your settings.
The Customizer : Complete Setup panel appears.
5. Press F3 (Exit).
The Customizer : System Parameters panel appears.

Discover System Resources

You can discover your system resources using Express Setup.

Run Express Setup

Express Setup discovers resources and stores their definitions in a system image. Express Setup starts after initial customization has completed.

Express Setup relies on SNMP, name lookup, and Netstat enablement. Ensure that these facilities are configured correctly for the [stack that you previously configured](#) (see page 138).

Note: Express Setup uses SNMP to discover IP nodes. If you have any special SNMP requirements for IP nodes, for example, nonstandard community names or a requirement to use a specific SNMP version, define them using the Maintain SNMP Installation Details option on the TCP/IP Administration Menu. The shortcut is /IPADMIN.S.

To run Express Setup

1. Exit from the Customizer : System Parameters panel if you have not already done so.

The Automation Services : Confirm Express Setup panel appears.

2. Select IP Express Setup.
3. Specify values in the System Image and Version fields. These values default to the local z/OS system name and the next available version number.
4. (Optional) Configure the \$RMEXPR6 control member:
 - a. Copy *dsnpref.NMC1.CC2DEXEC(\$RMEXPR6)* into *dsnpref.rname.TESTEXEC*.
 - b. Update the *dsnpref.rname.TESTEXEC(\$RMEXPR6)* specifications. (For example, comment out the resources you do not need to discover.)
 - c. Rename \$RMEXPR6, and use this name in the Control Member field.

Note: For an overview of what resources Express Setup builds when using the default \$RMEXPR6 control member, see the online help.

5. Set Load Image? to **YES**.

This system image is loaded after the discovery has completed.

6. Set the Create Application Name Definitions? field to **YES**.

Note: When the value is YES, application name definitions are created automatically for discovered address spaces that are important. You can implement additional application names manually later. For more information, see the *Implementation Guide*.

Note: If you are migrating, set this field to NO and migrate your application name definitions.

7. Press F6 (Action).

The Automation Services : Express Setup Status panel appears. This panel reports the progress of the resource discovery and the number of resources successfully discovered.

Note: The time taken to complete this process is determined by your site's configuration.

Access Express Setup After Logon

To access Express Setup after your first logon, enter **/RADMIN.AD.I** at the command prompt.

Note: For information about reviewing and administering the resources discovered by Express Setup, see the *Implementation Guide*.

Set Up the System Image to Load on Restart

Use this procedure to ensure that a system image is loaded during initialization.

Follow these steps:

1. Enter **/PARMS** at the command prompt.

The Customizer : Parameter Groups panel appears.

2. Enter **U** next to the \$RM AUTOIDS parameter group.

The AUTOIDS - Automation Identifiers panel appears.

3. Enter **?** in the System Image Name field.

The ResourceView : System Image List panel appears.

4. Select the System Image and Version you specified during Express Setup.

5. Press F6 (Action) if the system image is not already loaded.

Important! F6 (Action) replaces the currently loaded system image. If you do not want to load the system image now, skip this step.

6. Press F3 (File).

The system image loads each time the product region starts.

Initialization Failures

Fatal errors occur (for example, you are unable to log on) if either or both of the following are unavailable:

- Panel libraries
- MODS control files

Note: If the Panel libraries are missing, the system may display the N59005 message, which says that the \$MHMENU panel is not found. To retry, press F3, or to log off, press F4.

A Customizer parameter group always produces initialization log messages. The messages are echoed to the activity log. If a parameter group fails to initialize and you cannot log on to the region to display error messages, use CA SYSVIEW, SDSF, or an equivalent utility to display the activity log SYSOUT DD. The ddnames are LOG1 through to LOG9.

Resolve Initialization Failures

If you log on to a region where the initialization of a parameter group has failed, Customizer displays the System Initialization In Progress dialog. This dialog indicates progress and assists you with identifying and rectifying any problems by displaying the current initialization status and whether actions associated with parameter groups have failed.

Follow these steps:

1. Enter **S** next to List Only Failed Parameters.
2. Enter **L** next to a failed parameter group to view its log and look for error messages.
3. Use the message online help and the full activity log to determine the cause of the failure.
4. Make the necessary changes to the parameter group and press F6.
The parameter group changes are applied.
5. Press F3 to save the changes.

Parameter Group Actions

You can apply the following actions to listed parameter groups:

- **S** or **B** (Browse) to browse parameter group details.
- **H** (Help) to view the online help for a parameter group.
- **U** (Update) to update parameter group details.
- **AC** (Action) to action a parameter group.
- **L** (Log) to view the associated initialization and customization log.
- **I** (Ignore) to tell the system to ignore a failed parameter group and proceed to run dependent parameter groups. This action is not available when initializing for the first time.

Important! Ignoring parameter groups is not recommended. Consider carefully before applying this action.

- **SD** (Set Default) to reset the parameter group values to the default values.

Note: Press F1 (Help) for more information.

An action can only be performed against an already completed parameter group or a failed parameter group.

When you correct an error by updating an incorrect parameter group record, you must action that parameter group before processing can continue (unless you apply the Ignore action). To action the parameter group, do *one* of the following:

- Press F6 (Action) when you finish updating the parameter group.
- Apply **AC** (Action) to the listed parameter group.

Review Region Status

After completing your initial product customization, you should review the status of your region to ensure it is ready to be used.

To review the status of your region

1. Enter `/IPTEST` at the command prompt.
A summary of region configuration details appears.
2. Ensure that the information that appears is as expected based on the customization that you have performed in this chapter.

Note: Red text indicates an error and yellow text indicates a warning.

3. Address any errors or warnings by reviewing the customization steps you previously performed to ensure you have not missed any steps.

Note: For more information about how to perform a self-test, see the *Administration Guide*.

Perform Additional Customization

You have now completed the initial customization tasks for your product.

There are many other ways that you can customize your product, and they are described in the *Implementation Guide*.

Chapter 15: Completing Migration

The process to complete the migration includes tasks that you perform after you start your new product region.

This section contains the following topics:

[Knowledge Base Migration](#) (see page 149)

[MODS Migration](#) (see page 152)

[Panel Migration](#) (see page 154)

[OSCNTL File Migration](#) (see page 156)

[Migrate Baseline Data](#) (see page 156)

[Migrate IPLOG Records](#) (see page 158)

[Region Links to a Multisystem Network](#) (see page 158)

Note: If you are migrating from a version earlier than r11, [contact Technical Support](#) (see page 4).

Knowledge Base Migration

The knowledge base is where you store your resource definitions. System images, in which you define the resources a region manages, are part of the knowledge base.

Note: For more information about the knowledge base, see the *Reference Guide*.

As part of region setup, a knowledge base is created, comprising the following data sets:

- RAMDB
- ICOPANL

Migrate any existing data that you want to keep to this knowledge base.

Important! The IDCAMS REPRO command must never be used to manage the definitions in the knowledge base.

Migrate Your Existing Knowledge Base

If you are migrating multiple synchronized regions, you only perform this task for the first focal region. You do not have to perform this task when migrating subsequent regions because when you link the regions, the knowledge base is synchronized.

Important! Keep the old knowledge base until your new product regions are performing correctly.

Follow these steps:

1. Shut down the region using your existing knowledge base.
2. From the new product region, enter **/RAMUTIL.M**.
The RAMDB Migration Utility panel appears.
3. Perform the following steps:
 - a. Specify the data set name for your existing RAMDB in the Old RAMDB Data Set Name field.
The data set name is *dsnpref.rname*.RAMDB.
 - b. Specify **NO** in the Selective Migration field to migrate all definitions.
The utility migrates only customized definitions from the old knowledge base to the knowledge base in the new product region. Definitions that are not migrated are listed for further action.
 - c. Press F6 (Action) to display the Migration Statistics panel.
4. After migration has completed, perform the following steps:
 - a. Look for the components that have a non-zero value in the Not Copied column. (The utility does not copy a component if the component exists in the new knowledge base.)
You might have customized some of these components and want to copy them.
 - b. Enter **R** next to the components that you want to copy, and copy the records.
The copying options depend on whether a component contains [multiple objects](#) (see page 151), such as a system image, or is the [object itself](#) (see page 151), such as a user profile definition.
5. After you have copied the components, exit the migration utility.

Note: If you do not want to move directly from your established regions to the new product regions, you can run the two releases in parallel.

How to Copy Multi-Object Components

Important! The products use template images \$TEMPLAT 0001 through 0009 for the distribution of new and updated template definitions. Do not overwrite or replace them in the knowledge base.

If a component contains multiple objects, you operate on the component as a whole. You can perform the following actions:

- Merge the component in the old knowledge base into the component in this knowledge base. Only objects that do not exist in this knowledge base are migrated. Existing objects are unchanged.
- Overwrite the existing objects in this knowledge base with the objects in the old knowledge base. This operation does not affect any objects that are not in the old knowledge base.
- Replace the component in this knowledge base with the component in the old knowledge base.

Note: To migrate specific objects, see the activity log and use the RMMUAD05 messages to determine which objects have not been copied. You can then delete the appropriate objects and redo the migration by merging (to list only the RMMUAD05 messages in the log, enter **TEXT RMMUAD05**).

How to Copy Single-Object Components

For a component that is the object, do *one* of the following:

- Rename the component to create a copy of the component in this knowledge base using a different name.
- Overwrite the existing component in this knowledge base with the component in the old knowledge base.

Apply Updated Templates

After you have migrated your knowledge base, review the distributed templates.

Note: For information about changes to the distributed knowledge base, see the *Release Notes*.

Follow these steps:

1. Review the new templates to determine whether they are suitable for your requirements.
2. Enter **/RADMIN.T**.
The Template Definition menu appears.
3. Select the appropriate option to list the definitions you want to review.
4. If you use any template image except the default (as specified in the OPSYSIDS parameter group), copy the required definitions to your working template images.

Important! When you copy definitions from the distributed template images to your working template images, you can replace your working definition with a distributed definition of the same name. If you want to retain your working definition, make a copy of the definition beforehand.

If you want to copy all the new definitions, perform the following steps:

- a. Copy the template image (enter **/RADMIN.T.I**).
- b. Enter **C** next to the distributed image to merge the distributed template image with the target image.
- c. Specify **YES** in the Enter 'YES' to OVERLAY Like-named Components field.

If you want to copy changed definitions, copy them one by one.

5. If you want to apply a new template to all the resource definitions (in one or more system images) that use it, use the **AP** (Apply Template) action code. Specify **RESET** and **REPLACE** to ensure that the template is applied in full. If you want to retain an old definition, make a copy of the definition before you apply the template.

MODS Migration

Note: If you have not created your own MODS file, or individual MODS entities, do not perform this step.

MODS File

The format of the MODS file is unchanged. If you have a MODS file containing only user-defined MODS entities that you want to keep, copy the entire file to the file for the new region using the IDCAMS REPRO command.

Note: The MODSFILES parameter group in Customizer controls the allocation of MODS data sets. For more information, enter **/PARMS** on any panel, select \$NM MODSFILES, and press F1 (Help).

Copy MODS Definitions

The following entities are stored in the MODS file:

- Application definitions
- Command definitions
- Criteria definitions
- Help definitions
- List definitions
- Menu definitions
- Message definitions
- Print Services definitions
- Report definitions
- Table definitions

Note: Help alias entities are no longer supported. If you have installation-defined help aliases, convert them to a help page, and code the .cp macro to copy the original member. For more information about help macros, see the *Managed Object Development Services Guide*.

To copy MODS entities from your previous MODS file to your current one

Important! Copy only installation-defined entities. Do not copy distributed entities.

1. Enter **/MODSADE** from any panel.
The MODS : Entity Administration Menu appears.
2. Type **C** at the prompt, specify the information to copy your entities from the MODSUSR data set used by the old region to the MODSUSR data set used by this region, and press Enter.
The MODS : Entity List panel appears.
3. Select the entities that you want to copy, and press Enter.

Panel Migration

Note: If you have not created your own panel file, or individual panel entities, do not perform this step.

Installation-Defined Panel Library

The format of the panel library is unchanged. If you have a panel library that contains only user-defined panel definitions that you want to keep, copy the entire file to the file for the new region. Use the IDCAMS REPRO command to copy the file.

Notes:

- You do not need to migrate installation-defined icon panels in the ICOPANL file. These panels are recreated during the knowledge base migration.
- The PANELLIBS parameter group in Customizer controls the allocation of panels data sets. For more information, enter **/PARMS** from any panel, select \$NM PANELLIBS, and press F1 (Help).

Individual Panels

If you have installation-defined panel definitions in the same panel library as distributed panel definitions, you can copy the individual panel definitions to a panel library for the new region.

Important! Only copy installation-defined panel definitions. Do not copy distributed panel definitions.

Copy Panel Definitions

You must copy the required panel definitions to the panel library in your new product region.

Follow these steps:

1. Define a temporary panel library for your old panels using the following steps:
 - a. Enter **/MODSAD.P**.
The MODS : Panel Library Maintenance Menu appears.
 - b. Select **L - Library Definitions**.
The MODS : Library Definition Menu appears.
 - c. Select **A - Allocate, Open, and Define Library**, and specify a library name (for example, OLDPANLS) and the data set name where your old panels are located. Optionally, specify a description.
A temporary panels library is defined.
 - d. Press F3 (Exit) to return to the MODS : Panel Library Maintenance Menu.
2. Copy the panels using the following steps:
 - a. Select **C - Copy Panel(s)**, and specify the From library as the library name you just defined (for example OLDPANLS) and the To library as the target panels library name.
If you leave the Panel Name field empty, the MODS : Panel Copy List appears, showing the panels in the From library.
 - b. Use the **C** (Copy) or **R** (Replace) action against the panels you want to copy.
Note: For more information, press F1 (Help).
 - c. When all requested panels have been copied, press F3 (Exit) to return to the MODS : Panel Library Maintenance Menu.
3. Delete the temporary panel library definition using the following steps:
 - a. Select **L - Library Definitions**.
The MODS : Library Definition Menu appears.
 - b. Select **U - Remove Library Definition, Close and Unallocate**, and specify the library name (for example OLDPANLS).
The temporary panels library definition is removed.

Note: For more information about the MODS Panel Library Maintenance facility, see the *Managed Object Development Services Guide*.

OSCNTL File Migration

The format of the OSCNTL file is unchanged. If your existing OSCNTL file contains installation-defined ASN.1 maps, recompile them in the new product region.

Add the data set containing the map source to the COMMANDS concatenation in your new region. To compile a map, use the Compile Map option of Mapping Services. To access the Mapping Services Primary Menu, enter **/MAPMENU** from any panel.

Note: For more information about Mapping Services, see the *Managed Object Development Services Guide*.

Migrate Baseline Data

(Optional) Baseline data from releases before r12 is stored in VFS. If you want to use this data, migrate the data to the MSDB VSAM file at your earliest convenience.

Note: For baseline data from r12 (which is in MSDB), the S06MIGRT setup job handles the migration.

Follow these steps:

1. Ensure that the size of MSDB is at least as large as the size allocated to the existing VFS.

Note: For the cluster definition of MSDB, see the NMC1.*rname*.JCL(S01LCALC) data set member. If you require a larger size, update the RECORDS parameter. The MSDB parameter group specifies this file.

2. Log on to your new region.
3. Enter CMD at the command prompt.

A command entry panel appears.

4. Enter the following command:

```
SUBMIT BSYS $CAPKCAL $DFDBPKG DFDBMIGRATE FDSN=vfs_data_set RESET=YES
```

The migration starts as a background process, enabling you to perform other tasks. When the process completes, a DFDBPKG25 message is written to the activity log. The log also contains other messages that records the process. The MSDB file is cleared, and the data is migrated.

\$CAPKCAL \$DFDBPKG DFDBMIGRATE Procedure—Migrate Baseline Data

The \$CAPKCAL \$DFDBPKG DFDBMIGRATE procedure migrates baseline data from VFS to MSDB.

The procedure has the following format:

```
$CAPKCAL $DFDBPKG DFDBMIGRATE { FFID=vfs_file_id | FDSN=data_set_name }  
    [ TFID=MSDB | TDSN=data_set_name ]  
    [ RESET={ NO | YES } ]  
    [ FORCE={ NO | YES } ]  
    [ CLEANUP={ NO | YES } ]
```

FFID or FDSN

Specifies the file ID or data set name of the VFS that contains the data to be migrated.

TFID or TDSN

Specifies the file ID or data set name of the MSDB file to which data is to be migrated.

Default: TFID=MSDB

RESET

Specifies whether existing baseline data is deleted from the MSDB before migration.

Default: NO

FORCE

Specifies whether to migrate the data even when the MSDB contains baseline data. If data exists for an attribute in both the VFS and the MSDB, the data in the MSDB is overwritten. That is, any data collected for that attribute in the MSDB is lost.

Default: NO

CLEANUP

Specifies whether to delete the migrated baseline data from the VFS.

Default: NO

Migrate IPLOG Records

(Optional) The format of IPLOG has changed. If you want to use the records, migrate them. To migrate IPLOG records, do not use IDCAMS REPRO.

Follow these steps:

1. Log on to your new region.
2. Enter CMD at the command prompt.

A command entry panel appears.

3. Enter the following command:

```
SUBMIT BSYS $IPL082Z ACTION=IMPORT DSNAME=old_iplog_data_set_name
```

Note: Migration of large numbers of records can take significant time, and performance depends on the I/O subsystems used.

Region Links to a Multisystem Network

If the region you are migrating is to be [synchronized with other regions](#) (see page 21), review the sections that follow.

Important! Unlink your existing region from the multisystem network before upgrading it. Then, relink the upgraded region to the multisystem network.

Important Considerations Prior to Linking

Consider the following before linking:

- The first region linked in migration mode must be used to perform all monitoring, command, and control functions across the entire multisystem environment.
- Migration mode does not support database synchronization between the old and new product regions. We recommend that you do not perform database maintenance while operating in migration mode.
- If database maintenance is unavoidable, make changes in an old region, and again in a new region so that all linked regions have the changes propagated to them.

Link in Migration Mode

You can link your first migrated product region to your existing product regions in migration mode.

Migration mode lets you migrate your existing product regions in an orderly fashion while maintaining visibility and control of your entire multisystem environment.

Notes:

- Apply the relevant maintenance to your product region, including checking [software requirements](#) (see page 13) and [multisystem network migration](#) (see page 23).
- If you have specified the NMSUP parameter in the RUNSYSIN member for your existing product region, specify this parameter in the RUNSYSIN member for your new product region. The NMSUP parameter can be used to decrease the number of unique background user IDs that must be defined if you are using an external security package.

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

Follow these steps:

1. Enter `=/MADMIN.MM` in the new product region.
2. Specify the name of an existing focal region in your multisystem network.
3. Press F6 (Action).

Migrate Subsequent Regions

When a subsequent product region is migrated to the new release, you can use this procedure to link it to the first migrated product region.

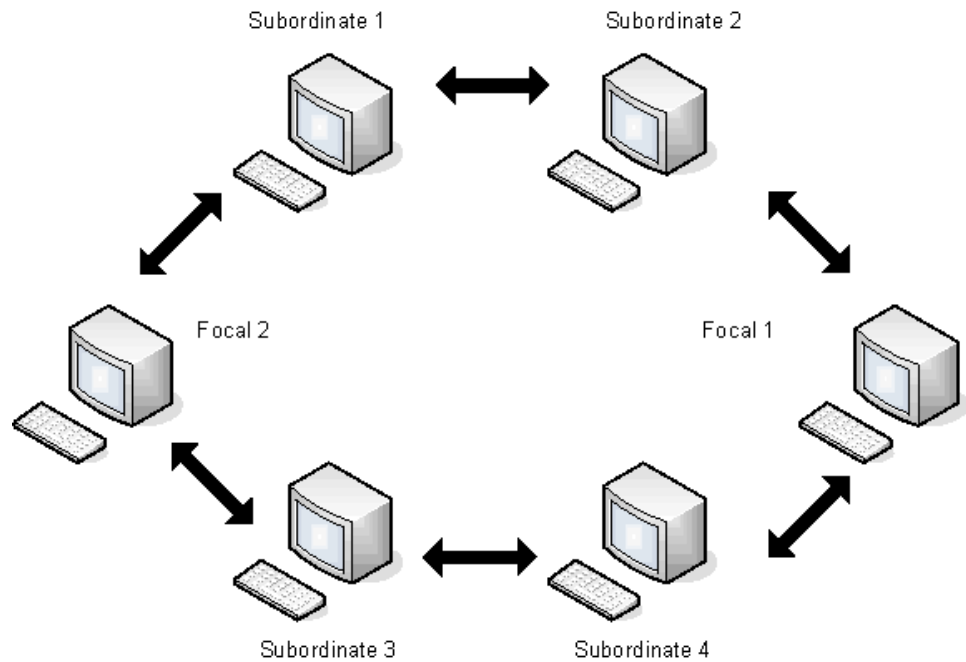
Follow these steps:

1. Enter `=/MADMIN.SD`.
2. Specify the first Release 12.1 product region as the remote region.
3. Specify the role for this region (focal or subordinate).
4. Press F6 (Action).
5. Repeat these steps for all of the remaining subordinate and focal regions. Migrate is the focal region that you first linked using migration mode last.

This migration sequence retains the visibility to the multisystem network throughout the migration process.

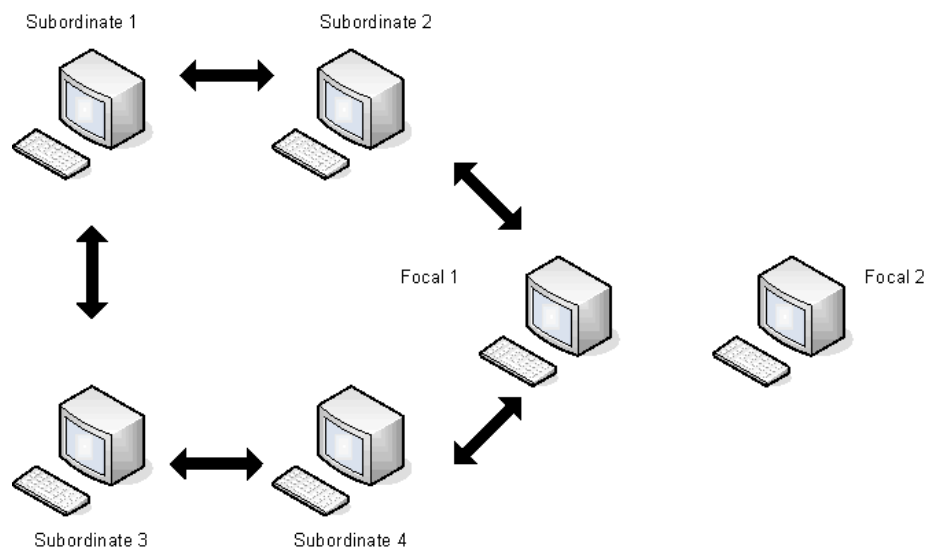
A Multisystem Network Migration Example

The following diagram shows a multisystem network with two focal regions and four subordinate regions:



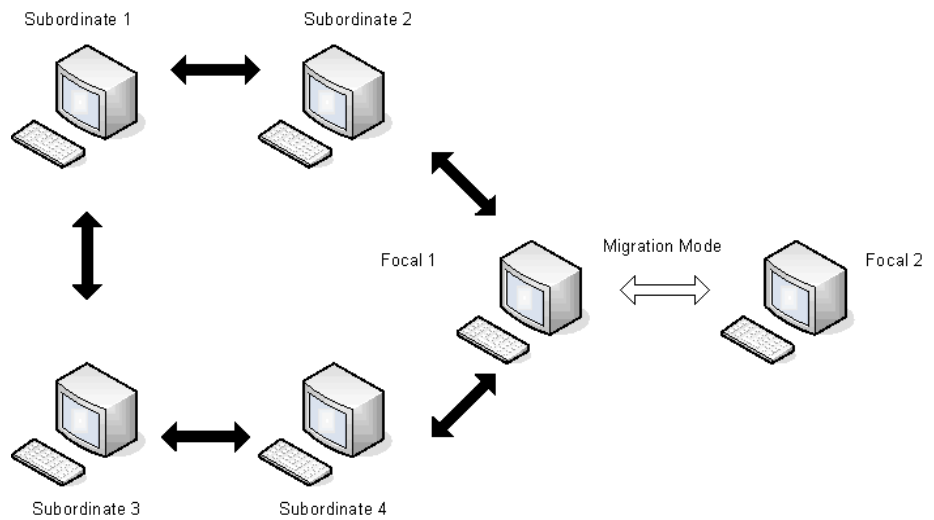
To migrate a multisystem network

1. Unlink Focal 2 from the existing multisystem network, as shown in the following diagram:

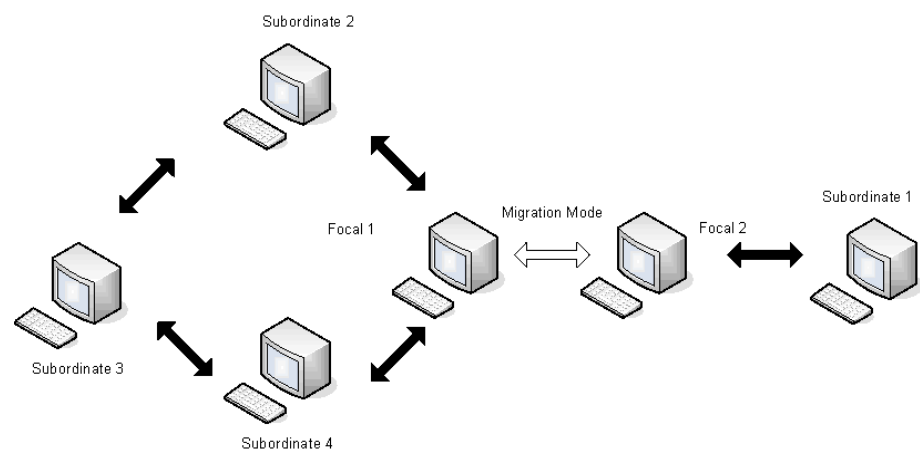


2. Upgrade Focal 2 to Release 12.1.

3. Link Focal 2 to Focal 1 in migration mode, as shown in the following diagram:



4. Unlink Subordinate 1 from the multisystem network and upgrade it to Release 12.1.
5. Link and synchronize Subordinate 1 to Focal 2, as shown in the following diagram:



6. Repeat Steps 4 and 5 for Subordinates 2-4 and Focal 1.

Appendix A: Worksheets

This section contains the following topics:

[Preparation Worksheets](#) (see page 163)

[Post-installation Worksheet](#) (see page 175)

Preparation Worksheets

During the installation and setup process, you enter values that are used to do the following:

- Allocate data sets.
- Set initial parameters.
- Prepare for the use of your product.

You can print out the worksheets in this section to record the values needed for your site when installing the product.

Note: For information about data sets, see the *Reference Guide*.

Installation

This worksheet helps you gather information required for installation.

Job Information

Gather the following job information:

Batch job class

Record the value that your site uses here:

Class = _____

Default: A

Batch job class for tape mounts

(Tape only) Record the value that your site uses here:

Class = _____

Instructions to operator

Record any instructions here:

Tape Unloading

If you are installing from tape, gather the following information related to tape unloading:

Tape unit

Record the value that your site uses for UNIT=*?device_in* here:

UNIT = _____

Example: CART

Tape volume serial number

Record the value that your site uses for VOL=SER=*?tapeser* here:

VOL=SER = _____

Example: C2D760

Tape expiry date

Record the values that your site uses here:

Expiry Date = _____

Example: 98000

Gather the following information related to the DASD to which the software is unloaded:

Data set prefix

Do not include the name of your planned product region.

Limits: Maximum 29 characters

Record the value that your site uses here:

?dsnpref = _____

DASD unit

Record the value that your site uses here:

?device_out = _____

DASD volume serial number

Record the value that your site uses here:

?volser = _____

Unload DASD

Gather the following information related to the DASD to which the software is unloaded:

Data set prefix

Do not include the name of your planned product region.

Limits: Maximum 29 characters

Record the value that your site uses here:

?dsnpref = _____

DASD unit

Record the value that your site uses here:

?device_out = _____

DASD volume serial number

Record the value that your site uses here:

?volser = _____

Installation Parameters

Gather the following information related to installation parameters:

Allocation Parameters

Use these prefixes for high-level qualifiers for the different data set groups.

Record the values that your site uses here:

SMP/E Target

Data Set Prefix = _____

Management class = _____

Storage class = _____

Volume serial number = _____

Unit = _____

SMP/E Distribution

Data Set Prefix = _____

Management class = _____

Storage class = _____

Volume serial number = _____

Unit = _____

SMP/E Libraries

Data Set Prefix = _____

Management class = _____

Storage class = _____

Volume serial number = _____

Unit = _____

SMP/E CSI

Data Set Prefix = _____

Management class = _____

Storage class = _____

Volume serial number = _____

SMPTLIB

Data Set Prefix = _____

Volume serial number = _____

Unit = _____

Language Environment Parameters

Record these language environment values:

Language Environment link-edit input 2

Record the value that your site uses here:

SCEEEND2 = _____

Default: CEE.SCEEEND2**Language Environment link-edit input**

Record the value that your site uses here:

SCEELIB = _____

Default: CEE.SCEELIB**Language Environment library**

Record the value that your site uses here:

SCEELKD = _____

Default: CEE.SCEELKD

System Programmer C routines

Record the value that your site uses here:

SCEESPC = _____

Default: CEE.SCEESPC

IBM macros

Record the value that your site uses here:

MODGEN = _____

Default: SYS1.MODGEN

Data set that contains the GIMZPOOL member

Record the value that your site uses here:

Default: SYS1.MACLIB

Region Setup

This worksheet helps you gather information required for region setup.

SOLVE Subsystem Interface Region

Gather the following information related to the SOLVE Subsystem Interface region:

Name of the SOLVE SSI started task (*ssiname*)

Record the value that your site uses here:

Default: SOLVESSI

Name of the SOLVE SSI SYSIN member

This member contains control statements for starting the SOLVE SSI.

Record the value that your site uses here:

SYSIN = _____

Default: SSISYSIN

Name of the optional SOLVE SSI parameter member

This member contains startup parameters for the SOLVE SSI. If omitted, startup parameters are included in the SOLVE SSI SYSIN member previously described.

Record the value that your site uses here:

PARAMETER = _____

Subsystem ID for a SOLVE SSI started task

Record the value that your site uses here:

SSID = _____

Default: SOLV

Prefix for SOLVE SSI data sets

Record the value that your site uses here:

Default: *dsnpref*

Name of the stack for EE packet processing (*stack_name* | NONE)

Identify the stack that is used for Enterprise Extender (EE) traffic. The value is the name of the stack job or started task.

PAEESTACK = _____

IPSec monitoring (NO | YES)

(IBM stacks only) If the stack is configured for IPSECURITY, determine whether you want to collect IPSec information:

IPSECNMI = ____

Product Region

Gather the following information about the product region:

Product region started task name (*rname*)

Record the value that your site uses here:

Default: NM

Product region SYSIN member name

Record the value that your site uses here:

SYSIN = _____

Default: RUNSYSIN

Primary VTAM ACB name for the product region

Record the value that your site uses here:

PRI = _____

Default: NM

Mixed case passwords

Specifies whether case is preserved (YES) or forced to uppercase (NO):

Default: NO

Security exit setting (NO|PARTSAF|NMSAF|NMSAFF|*lname*)

Record the value that your site uses here:

SEC = _____

Default: NO

Note: For more information about setting your security exit, see the *Security Guide*.

SYSOUT

Specifies SYSOUT subparameters. You can specify a class, a writer, and a form.

Default: *

CA Cross-Enterprise APM Interface

Specifies whether the region supports integration with CA Cross-Enterprise APM. If you specify YES, the following parameter is added to the *dsnpref.rname*.TESTEXEC(RUNSYSIN) member:

PPREF= 'PROD=APM'

Default: NO

Prefix for VSAM data sets local to the product region

Record the value that your site uses here:

Default: *dsnpref.rname*

Prefix for sequential data sets local to the product region

Record the value that your site uses here:

Default: *dsnpref.rname*

Prefix for TESTEXEC

Record the value that your site uses here:

Default: *dsnpref.rname*

Prefix for UAMS or full name of existing UAMS

Record the value that your site uses here:

Default: *dsnpref*

Prefix for shareable VSAM data sets

Record the value that your site uses here:

Default: *dsnpref.NMC1*

Prefix for shareable PARMLIB data sets

Record the value that your site uses here:

Default: *dsnpref.NMC1.PARMLIB*

AOM subsystem interface ID

Record the value that your site uses here:

AOMSSID = _____

Default: Domain ID of the region

Note: Verify that this value does not conflict with other subsystems. The AOM subsystem interface enables system message flow to the region.

AOM message suppression character

Record the value that your site uses here:

Default: /

AOM SSI command prefix string

Record the value that your site uses here:

Default: *domain_id>*

Note: If you use a command string prefix for other tasks, verify that this value is not in conflict with them.

External application ACB pool names

Full-screen terminal prefix

Record the value that your site uses here:

Default: NMMAF

LU1 terminal prefix

Record the value that your site uses here:

Default: NMMAV

VTAM Definitions

Gather the following information related to VTAM definitions:

VTAM major node name

Record the value that your site uses here:

Default: VTAMAPPL

System macro library

Record the value that your site uses here:

Default: SYS1.MACLIB

VTAM network definitions library

Record the value that your site uses here:

Default: SYS1.VTAMLST

VTAM macro library

Record the value that your site uses here:

Default: SYS1.SISTMAC1

VTAM load library

Record the value that your site uses here:

Default: SYS1.VTAMLIB

(Optional) External Interface Package (EIP) ACB Prefix

Record the value that your site uses here:

Default: NMTSO

TCP/IP Setup

Gather the TCP/IP setup information in the following worksheet:

Name and release of the TCP/IP software

Record the value that your site uses here:

IBM Communications Server

Gather the following information related to the IBM Communications Server:

Started task user ID for product region

Record the value that your site uses here:

Started task user ID for SOLVE SSI

Record the value that your site uses here:

PW.SRC data set name

Record the value that your site uses here:

Default: /etc/pw.src

Stack IP address

Record the value that your site uses here:

PROFILE.TCPIP data set name

Record the value that your site uses here:

FTP.DATA data set name

Record the value that your site uses here:

TCPIP.DATA data set name

Record the value that your site uses here:

CA TCPaccess CS

Gather the following information related to the CA TCPaccess CS:

IJTCFGxx member

Record the value that your site uses here:

DNRALCxx member

Record the value that your site uses here:

DNRHSTxx member

Record the value that your site uses here:

DNRCFGxx member

Record the value that your site uses here:

SNMCFGxx member

Record the value that your site uses here:

CA TCPaccess CS subsystem ID

Record the value that your site uses here:

Default: ACSS

CA TCPaccess CS Job Name

Record the value that your site uses here:

PARM data set name

Record the value that your site uses here:

Startup Tasks

This worksheet helps you gather information related to the startup tasks.

Initial administrator user ID

Record the value that your site uses here:

Initial administrator password

Record the value that your site uses here:

Port number for inbound connections (if you intend to use TCP/IP as a transport method for INMC links)

Record the value that your site uses here:

Default: 2636

Port number for WebCenter

Record the value that your site uses here:

Default: NONE

Post-installation Worksheet

After you have completed the installation and setup processes, you can record the data set names generated by the Install Utility for future reference.

You can print out the following worksheet now, and record this information as you progress through this guide.

Installation data set

Record the value generated by the Install Utility here:

Default: *dsnpref*.NMC1.CC2DJCL

Installation JCL data set

Record the value generated by the Install Utility here:

Default: *dsnpref*.NMC1.INSTALL.JCL

SOLVE SSI setup JCL data set

Record the value generated by the Install Utility here:

Default: *dsnpref.NMC1.ssiname.JCL*

Product region setup JCL data set

Record the value generated by the Install Utility here:

Default: *dsnpref.NMC1.rname.JCL*

VTAM JCL data set

Record the value generated by the Install Utility here:

Default: *dsnpref.NMC1.VTAM.JCL*

Appendix B: Defining UNIX System Services Authorization

This section contains the following topics:

[USS Authorization Requirements](#) (see page 177)

[Set Up OMVS Segment](#) (see page 177)

USS Authorization Requirements

To complete this task you must have the following:

- Administrative access to your security package
- OMVS shell write privileges

To authorize a user, you can use one of the following:

- Default OMVS segment
- Specific OMVS segment

More information:

[Define UNIX Authorization for Your Started Task User IDs](#) (see page 101)

Set Up OMVS Segment

Use this procedure to set up an OMVS segment.

Follow these steps:

1. Assign an OMVS UID number to each user ID. If your security administrator does *not* have a policy for assigning OMVS UID numbers, use a unique number.

Note: For more information about OMVS UID numbers, see the IBM *UNIX System Services Planning* guide.

2. Define the OMVS segment for the user. For a user ID *uuuuuuu* and UID number *nnn*, enter the following commands:

- For CA ACF2 for z/OS systems, enter the following commands:

```
SET PROFILE(USER) DIV(OMVS)
INSERT uuuuuuu UID(nnn) HOME(/) PROGRAM(/bin/sh)
```

- For CA Top Secret for z/OS systems, enter the following commands:

```
TSS ADD(uuuuuuu) HOME(/) OMVSPGM(/bin/sh) UID(nnn)
GROUP(OMVSGRP)
```

- For RACF systems, enter the following command:

```
ALU uuuuuuu OMVS(UID(nnn) HOME(/) PROGRAM(/bin/sh))
```

Note: The OMVS segment must contain a home directory (HOME) and a login shell (PROGRAM or OMVSPGM).

3. Complete this process for each user ID that you want to authorize. To confirm the contents of the OMVS segment, enter the following commands:

- For CA ACF2 for z/OS systems, enter the following commands:

```
SET PROFILE(USER) DIV(OMVS)
LIST uuuuuu
```

- For CA Top Secret for z/OS systems, enter the following command:

```
TSS LIS(uuuuuu) DATA(ALL)
```

- For RACF systems, enter the following command:

```
LISTUSER uuuuuu OMVS NORACF
```

4. Assign a home directory to each user ID, and ensure that it exists and that the UID has at least READ access to it.

You can use the UNIX root directory (/) as shown in Step 2, or you can use a customized home directory name.

For example, to set up a directory named /u/name for UID*nnn*, issue the following commands in the OMVS UNIX shell:

```
mkdir /u/name
chown nnn /u/name
chmod 777 /u/name
```

5. Confirm the owner and access to the directory by using the following command:

```
ls -ld /u/name
```

The following result appears:

```
drwxrwxrwx  2 user  group 8192 Sep 31 14:58 /u/name
```

Appendix C: Tape Format

The following topics provide information about the function modification identifiers (FMIDs) and details about the format of the tapes that you receive to install your product.

Note: The tapes contain all files for all products in the CA Mainframe Network Management family of products. Only some of the files apply to your product, and therefore, only the files necessary to install your product are unloaded.

This section contains the following topics:

[FMID Descriptions](#) (see page 179)

[Format of Cartridge VOLSER C2D760](#) (see page 180)

FMID Descriptions

This product has the following FMIDs, which are codes that identify the release levels of a product:

CC11C10

Is the FMID for TCP/IP Services.

CC17C10

Is the FMID for File Transfer Services.

CC18C10

Is the FMID for SNA Automation Services.

CC2AC10

Is the FMID for SNA Services.

CC2D76E

Is the FMID for PDSE Services (ME).

CC2D76H

Is the FMID for Health Checker (HC).

CC2D760

Is the FMID for Management Services (MS).

CC2D76R

Is the FMID for ReportCenter.

CDEMC10

Is the FMID for FTS Services.

Format of Cartridge VOLSER C2D760

This table lists the file sequence numbers, data set names, and data set contents for the first tape.

Files	DSN	Contents
1	CAI.SAMPJCL	Installation and maintenance JCL members
2	CAI.SMPMCS	Modification control statements (MCSs) containing functions and all published SYSMODs for those functions
3	CAI.CC2D76H.F1	++DATA for CC2D76H (RECFM=FB)
4	CAI.CC2D76H.F2	++EXEC for CC2D76H
5	CAI.CC2D76H.F3	++MSG for CC2D76H
6	CAI.CC2D76H.F4	++PNL for CC2D76H
7	CAI.CC2D76H.F5	++SAMP for CC2D76H
8	CAI.CC2D76H.F6	++SKL for CC2D76H
9	CAI.CC2D76H.F7	++SKL for CC2D76H
10	CAI.CC2D76H.F8	NCAL-linked MODS for CC2D76H
11	CAI.CC2D760.F1	++CLIST for CC2D760
12	CAI.CC2D760.F2	++DATA for CC2D760 (RECFM=VB)
13	CAI.CC2D760.F3	++MAC for CC2D760 (Assembler)
14	CAI.CC2D760.F4	++MAC for CC2D760 (Assembler)
15	CAI.CC2D760.F5	++MAC for CC2D760
16	CAI.CC2D760.F6	++MAC for CC2D760 (OML)
17	CAI.CC2D760.F7	++MAC for CC2D760 (REXX)
18	CAI.CC2D760.F8	NCAL-linked MODS for CC2D760
19	CAI.CC2D760.F9	NCAL-linked MODS for CC2D760
20	CAI.CC2D760.F10	++PROGRAM for CC2D760
21	CAI.CC2D760.F11	++SAMP for CC2D760

Files	DSN	Contents
22	CAI.CC2D760.F12	++SAMP for CC2D760
23	CAI.CC2D760.F13	++SAMP for CC2D760
24	CAI.CC2D760.F14	++SAMP for CC2D760
25	CAI.CC2D760.F15	++SAMP for CC2D760
26	CAI.CC2D760.F16	++SRC for CC2D760
27	CAI.CC11C10.F1	++DATA for CC11C10 (RECFM=VB)
28	CAI.CC11C10.F2	++MAC for CC11C10
29	CAI.CC11C10.F3	++MAC for CC11C10 (OML)
30	CAI.CC11C10.F4	XML data for CA MSM
31	CAI.CC17C10.F1	++DATA for CC17C10 (RECFM=VB)
32	CAI.CC17C10.F2	++MAC for CC17C10
33	CAI.CC17C10.F3	++MAC for CC17C10 (Assembler)
34	CAI.CC17C10.F4	++MAC for CC17C10 (OML)
35	CAI.CC17C10.F5	XML data for CA MSM
36	CAI.CC17C10.F6	++SAMP for CC17C10
37	CAI.CC17C10.F7	++SAMP for CC17C10
38	CAI.CC17C10.F7	++SAMP for CC17C10
39	CAI.CC18C10.F1	++DATA for CC18C10 (RECFM=FB)
40	CAI.CC18C10.F2	++DATA for CC18C10 (RECFM=VB)
41	CAI.CC18C10.F3	++MAC for CC18C10
42	CAI.CC18C10.F4	++MAC for CC18C10 (OML)
43	CAI.CC18C10.F5	XML data for CA MSM
44	CAI.CC2AC10.F1	++DATA for CC2AC10 (RECFM=VB)
45	CAI.CC2AC10.F2	++MAC for CC2AC10
46	CAI.CC2AC10.F3	++MAC for CC2AC10 (OML)
47	CAI.CC2AC10.F4	XML data for CA MSM
48	CAI.CC2AC10.F5	++SAMP for CC2AC10
49	CAI.CDEMC10.F1	++CLIST for CDEMC10
50	CAI.CDEMC10.F2	++DATA for CDEMC10 (RECFM=VB)
51	CAI.CDEMC10.F3	++MAC for CDEMC10

Files	DSN	Contents
52	CAI.CDEMC10.F4	++MAC for CDEMC10 (OML)
53	CAI.CDEMC10.F5	++MSG for CDEMC10
54	CAI.CDEMC10.F6	++PAN for CDEMC10
55	CAI.CDEMC10.F7	XML data for CA MSM
56	CAI.CC2D76E.F1	NCAL-linked MODS for CC2D76E
57	CAI.CC2D76R.F1	++HFS for CC2D76R
58	CAI.CC2D76R.F2	++SHELLSCR for CC2D76R

Index

\$

\$CAPKCAL \$DFDBPKG DFDBMIGRATE procedure • 157

A

access
 login • 34
allocate and mount • 43
application name definitions • 143
application names, VTAM • 125

B

baselines • 156

C

CA Auditor, setting up • 125
CA Common Services • 15
CA MSM usage scenarios • 26
CA NetSpy, implementing • 142
CA TCPaccess CS
 subsystem ID • 138
communications server for SMF records, enabling • 99
Communications Server, IBM
 IPSec Network Management Interface • 103
 prefix.PW.SRC data set • 98
 SNA Network Management Interface • 102
consoles, assigning • 124
contacting technical support • 4
copy files to USS directory • 46, 47, 50
customer support, contacting • 4
Customizer parameter groups
 EXTAPPLS • 142
 MSDB • 156
 NETSPYLINKS • 142
 OPSYSIDS • 138
 SOCKETS • 138
 SYSTEMID • 138

D

data sets
 allocate region-specific (local) • 92
download

files using ESD • 39
options • 46
to mainframe through a PC • 50
using batch JCL • 47

E

ESD (Electronic Software Delivery)
 space requirement • 17
 USS access • 37
exit, CA TCPaccess CS exit • 109
Express Setup • 143
EXTAPPLS parameter group • 142
external HOLDDATA • 61

F

FMIDs • 179
free space • 42

G

gathering information in preparation for installation
 and setup • 163
GIMUNZIP utility • 52

H

hash setting • 52
high-level qualifier • 52
HOLDDATA • 61

I

IBM Communications Server, TCPIP.DATA data set
 name • 138
implementation
 CA NetSpy • 142
 operating system identifiers parameters • 138
 system ID parameters • 138
 TCP/IP sockets interface • 138
 WebCenter parameters • 140
initialization
 failures • 145
 INI file • 21
 setup types • 136
installation
 generating install jobs • 55
 JCL • 54, 55

- required information • 163
- setup process • 163
- installing
 - from Pax-Enhanced ESD • 37
 - from tape • 71
- Integrated Cryptographic Services Facility (ICSF) • 52
- internal HOLDDATA • 61
- IPSec Network Management Interface • 103

J

- Java version support • 52
- JCL jobs
 - installation • 54, 55

K

- knowledge base
 - migrating • 149

M

- maintenance • 59
 - applying directly to RAMDB • 65
 - backing up RAMDB • 65
 - RAMDB • 64
 - restoring RAMDB • 66
 - SMP fixes • 59
- migrations
 - baselines • 156
 - INI file • 21
 - knowledge base • 149
 - MODS • 152
 - OSCNTRL file • 156
 - panels • 154
- MODS, migrating • 152
- MSDB definition • 156
- multi-object components • 151

N

- NETSPYLINKS parameter group • 142
- NETSTAT interface, enabling • 97
- NPF member, reviewing • 127

O

- operating system identifiers parameters • 138
- OPYSIDS parameter group • 138
- OSA, setting up SF support • 122
- OSCNTRL file, migrating • 156

P

- panels, migrating • 154
- parameters
 - operating system identifiers • 138
 - system ID • 138
 - WebCenter • 140
- partitioned data sets, loading • 92
- pax ESD procedure
 - copy product files • 46
 - create product directory • 51
 - download files • 39
 - set up USS directory • 42
- pax file
 - copy files to USS directory • 46, 47, 50
- port number • 138
- procedures, \$CAPKCAL \$DFDBPKG DFDBMIGRATE • 157
- process overview • 37
- product download window • 39
- product regions
 - setup • 92
 - starting • 130
 - stopping • 130
- product-level directory • 51

R

- RAMDB
 - maintenance • 65
- read me • 52
- regions
 - product • 92
 - setup, product selection • 92
- requirements
 - security • 16
 - software • 13
 - storage • 17
- restart SOLVE SSI region • 130
- reviewing
 - NPF member • 127
 - SAF member • 127

S

- SAF member, reviewing • 127
- sample jobs • 47, 51
 - CAtoMainframe.txt • 47
 - Unpackage.txt • 51
- security

- access, checking • 16
- IPSec Network Management Interface • 104
- requirements • 16
- SNA Network Management Interface • 102
- setting up CA Auditor • 125
- setup
 - express • 143
 - product regions • 92
 - subsystem identifiers • 123
 - subsystem interfaces • 90
 - system image • 144
 - types • 136
- sharing a SOLVE SSI region • 90
- single-object components • 151
- SMF records, generating • 112
- SMP fixes • 59
- SMP/E
 - GIMUNZIP utility • 52
- SNA Network Management Interface • 102
- SNMP
 - agent • 98
 - collecting data from CA TCPaccess • 113
 - query engine • 98
- SOCKETS parameter group • 138
- SOLVE SSI
 - as common component • 90
 - configuring • 97
 - methods of specifying region • 90
 - sharing a region • 90
 - specifying • 90
- SOLVE SSI region
 - restarting • 130
 - starting • 129
 - stopping • 129
- start product region • 130
- start SOLVE SSI region • 129
- started task JCL • 117
- startup • 130
- stop product region • 130
- stop SOLVE SSI region • 129
- storage requirements • 17
- subsystem identifiers, set up • 123
- subsystem interfaces, specify • 90
- support, contacting • 4
- system ID parameters • 138
- system image
 - setting up • 144
- system symbols • 119, 120, 121, 122, 135
- SYSTEMID parameter group • 138

T

- tape, installing from • 71
- TCP/IP interface, z/OS • 138
- technical support, contacting • 4

U

- UAMS
 - administrator, initial • 131
- UNIX System Services (USS)
 - access requirements • 37, 42
 - directory cleanup • 57
 - directory structure • 42
- UNIX System Services (USS) shell • 97
- UNZIPJCL • 52
- updated templates, applying • 152
- user IDs
 - adding • 131

V

- VTAM
 - applications, defining • 125

W

- WebCenter
 - clearing the browser cache • 140
 - parameters • 140
 - port number, defining • 140
 - third-party products recommended • 14
- worksheets • 20
 - installation information • 164
 - region setup information • 168

Z

- z/OS environment, TCP/IP interface • 138