IBM Copy Services Manager
Version 6 Release 2

Installation and Configuration Guide

IBM

Note:

Before using this information and the product it supports, read the information in "Notices" on page 59.

Edition notice

This edition applies to Version 6, Release 2 , Modification 6 of IBM® Copy Services Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Tables

About this guide

This guide provides task-oriented installation and configuration information for IBM Copy Services Manager.

The Copy Services Manager family of products consists of the following licenses:

- IBM Copy Services Manager
- IBM Copy Services Manager for z Systems®
- IBM Copy Services Manager Basic Edition for z Systems

For z/OS installation: This guide is a supplement to the *IBM Copy Services Manager Program Directory* and the *IBM Copy Services Manager Basic Edition Program Directory* and focuses on the configuration and post installation steps that you must run after the SMP/E installation.

Who should read this guide

This publication is for administrators who install and configure IBM Copy Services Manager.

Administrators should be familiar with the following topics:

- Copy services concepts
- General principles of IBM AIX®, Linux, Microsoft Windows, and the z/OS® operating systems
- Simple Network Management Protocol (SNMP) concepts
- Storage area network (SAN) concepts

Conventions used in this guide

Explanations are provided about the conventions that are used in this publication.

This publication uses several conventions for special terms and actions, and for operating system-dependent commands and paths.

The following typeface conventions are used in this publication:

Bold

- Flags that display with text
- Graphical user interface (GUI) elements (except for titles of windows and dialogs)
- Names of keys

Italic

- Variables
- Values that you must provide
- New terms
- Words and phrases that are emphasized
- Titles of documents

monospace

- Commands and command options
- Flags that display on a separate line
- Code examples and output
- Message text

- Names of files and directories
- Text strings that you must type, when they display within text
- Names of Java™ methods and classes
- HTML and XML tags that display `like this`, in monospace type

For syntax notations, remember the following details.

- In AIX, the prompt for the root user is #.
- In AIX and Linux, the commands are case-sensitive, so you must type commands exactly as they are shown.

Publications and related information

Product guides, other IBM publications, and websites contain information that relates to IBM Copy Services Manager.

To view a PDF file, you need Adobe Reader. You can download it at no charge from the Adobe website (get.adobe.com/reader/).

Online documentation

The IBM Copy Services Manager online product documentation (http://www-01.ibm.com/support/knowledgecenter/SSESK4) contains all of the information that is required to install, configure, and manage IBM Copy Services Manager. The online documentation is updated between product releases to provide the most current documentation.

Publications

You can order or download individual publications that have an order number from the IBM Publications Center website (www.ibm.com/shop/publications/order/).

Table 1. IBM Copy Services Manager product publications		
Title	**Description**	**Order number**
IBM Copy Services Manager Installation and Configuration Guide	This guide provides task-oriented information for anyone who installs and configures IBM Copy Services Manager.	V6.2.6 **SC27-8543-10** V6.2.5 **SC27-8543-09** V6.2.3 **SC27-8543-08** V6.2.2 **SC27-8543-07** V6.2.1 **SC27-8543-06** V6.2.0 **SC27-8543-05** V6.1.5 **SC27-8543-04** V6.1.4 **SC27-8543-03** V6.1.3 **SC27-8543-02** V6.1.2 **SC27-8543-01** V6.1.0 **SC27-8543-00**

Table 1. IBM Copy Services Manager product publications (continued)		
Title	**Description**	**Order number**
IBM Copy Services Manager User's Guide	This guide provides task-oriented information for users of IBM Copy Services Manager. Users should be familiar with the following topics • Copy Services concepts • General principles of IBM AIX, Linux, Windows, and the IBM z/OS operating systems • Simple Network Management Protocol (SNMP) concepts • Storage Area Network (SAN) concepts	V6.2.6 **SC27-8542-12** V6.2.5 **SC27-8542-11** V6.2.4 **SC27-8542-10** V6.2.3 **SC27-8542-09** V6.2.2 **SC27-8542-08** V6.2.1 **SC27-8542-07** V6.2.0 **SC27-8542-06** V6.1.5 **SC27-8542-05** V6.1.4 **SC27-8542-04** V6.1.3 **SC27-8542-03** V6.1.2 **SC27-8542-02** V6.1.1 **SC27-8542-01** V6.1.0 **SC27-8542-00**
IBM Copy Services Manager Command-line Interface User's Guide	This guide provides information for customizing and using the command-line interface for IBM Copy Services Manager. This guide provides information for customizing and using the command-line interface for IBM Copy Services Manager.	V6.2.5 **SC27-8998-06** V6.2.4 **SC27-8998-05** V6.2.3 **SC27-8998-04** V6.2.2 **SC27-8998-03** V6.2.1 **SC27-8998-02** V6.2.0 **SC27-8998-01** V6.1.5 **SC27-8998-00**
IBM Copy Services Manager z/OS FlashCopy Manager User's Guide	This guide provides task-oriented information for those who administer FlashCopy® operations in a z/OS environment.	V6.2.5 **SC27-8032-05** V6.2.3 **SC27-8032-04** V6.2.2 **SC27-8032-03** V6.2.0 **SC27-8032-02** V6.1.5 **SC27-8032-01** V6.1.3 **SC27-8032-00**
IBM Copy Services Manager Release Notes	This document contains the release notes in support of IBM Copy Services Manager.	Search on IBM Copy Services Manager at IBM Fix Central (www.ibm.com/support/fixcentral) to locate and download the Release Notes® related to your product version.

Table 1. IBM Copy Services Manager product publications (continued)		
Title	**Description**	**Order number**
IBM Copy Services Manager for z Systems Program Directory and *IBM Copy Services Manager Basic Edition for z Systems Program Directory*	These program directories are intended for system programmers who are responsible for program installation and maintenance. They contain information about the material and procedures associated with the installation of IBM Copy Services Manager for z Systems and IBM Copy Services Manager Basic Edition for z Systems.	*IBM Copy Services Manager for z Systems Program Directory* V6.2.5 **GI13-4517-08** V6.2.3 **GI13-4517-07** V6.2.2 **GI13-4517-06** V6.2.1 **GI13-4517-05** V6.2.0 **GI13-4517-04** V6.1.4 **GI13-4517-03** V6.1.3 **GI13-4517-02** V6.1.1 **GI13-4517-01** V6.1.0 **GI13-4517-00** *IBM Copy Services Manager Basic Edition for z Systems Program Directory* V6.2.5 **GI13-4518-08** V6.2.3 **GI13-4518-07** V6.2.2 **GI13-4518-06** V6.2.1 **GI13-4518-05** V6.2.0 **GI13-4518-04** V6.1.4 **GI13-4518-03** V6.1.3 **GI13-4518-02** V6.1.1 **GI13-4518-01** V6.1.0 **GI13-4518-00**
Program Directory for IBM Copy Services Manager FlashCopy Manager for IBM Copy Services Manager for z Systems	This guide is intended for the system programmer or storage administrator of the IBM Copy Services Manager z/OS FlashCopy Manager utility.	V6.2.5 **GI11-2904-08** V6.2.3 **GI11-2904-07** V6.2.2 **GI11-2904-05** V6.2.1 **GI11-2904-04** V6.2.0 **GI11-2904-03** V6.1.4 **GI11-2904-02** V6.1.3 **GI11-2904-01**
IBM DSCLI on z/OS Program Directory	This program directory is intended for system programmers who are responsible for program installation and maintenance. It contains information about the material and procedures associated with the installation of the IBM Copy Services Manager on the DS8000® HMC for access to the DS8000 CLI.	V6.2.5 **GI13-3563-05** V6.2.3 **GI13-3563-04** V6.2.2 **GI13-3563-03** V6.2.1 **GI13-3563-02** V6.2.0 **GI13-3563-01** V6.1.4 **GI13-3563-00**

Related websites

View the websites in the following table to get more information about IBM Copy Services Manager.

Table 2. IBM Copy Services Manager related websites	
Title	**Description**
IBM website (ibm.com®)	Find more information about IBM products and services.

Table 2. IBM Copy Services Manager related websites (continued)	
Title	**Description**
IBM Support Portal website (www.ibm.com/support/home)	Find support-related information such as downloads, documentation, troubleshooting, and service requests and PMRs.
Copy Services Manager Support Portal (https://www.ibm.com/support/home/product/10000480/IBM_Copy_Services_Manager)	Find technical support information that is specific to IBM Copy Services Manager.
IBM Directory of Worldwide Contacts website (www.ibm.com/planetwide)	Find contact information for general inquiries, technical support, and hardware and software support by country.
IBM Redbooks® website (www.redbooks.ibm.com/)	Find technical information developed and published by IBM International Technical Support Organization (ITSO).
IBM System Storage® Interoperation Center (SSIC) website (www.ibm.com/systems/support/storage/config/ssic)	Find information about supported host system models, operating systems, adapters, and switches.
IBM Fix Central (www.ibm.com/support/fixcentral)	Find fixes and updates for your system's software, hardware, and operating system.

Sending comments

Your feedback is important in helping to provide the most accurate and highest quality information.

To submit any comments about this publication or any other IBM storage product documentation:

- Send your comments by email to starpubs@us.ibm.com. Be sure to include the following information:
  - Exact publication title and version
  - Publication form number (for example, GA32-1234-00)
  - Page, table, or illustration numbers that you are commenting on
  - A detailed description of any information that should be changed

Contacting IBM Software Support

You can contact IBM Software Support by phone, and you can register for support notifications at the technical support website.

- Go to the Copy Services Manager technical support website at Copy Services Manager Support Portal (https://www.ibm.com/support/home/product/10000480/IBM_Copy_Services_Manager).

  To receive future support notifications, sign in under **Subscribe to support notifications**. You are required to enter your IBM ID and password. After you are authenticated, you can configure your subscription for Copy Services Manager technical support website updates.

You can also review the *IBM Software Support Handbook,* which is available at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

The support website offers extensive information, including a guide to support services; frequently asked questions (FAQs); and documentation for all IBM Software products, including Redbooks and white papers. Translated documents are also available for some products.

When you contact IBM Software Support, be prepared to provide identification information for your company so that support personnel can readily assist you. Company identification information might also be needed to access various online services available on the website. See "Reporting a problem" on page xii.

Reporting a problem

Provide the IBM Support Center with information about the problems that you report.

Have the following information ready when you report a problem:

- The IBM Copy Services Manager version, release, modification, and service level number.
- The communication protocol (for example, TCP/IP), version, and release number that you are using.
- The activity that you were doing when the problem occurred, listing the steps that you followed before the problem occurred.
- The job log output for any failing IBM Copy Services Manager jobs.
- The exact text of any error messages.

Summary of changes

The following functions are introduced in IBM Copy Services Manager Version 6.2.6:

Version 6, Release 2, Modification 6

This table provides the current technical changes and enhancements to Copy Services Manager as of June 2019.

Table 3. Summary of changes in Copy Services Manager Version 6.2.6 (June 2019)

Function or feature	Description
Several minor updates have been made throughout the guide to clarify or provide additional information.	See the left margin revision indicators for changes in the 6.2.6 version of this guide.

Chapter 1. Planning considerations and installation prerequisites

These are the prerequisite system requirements that you need to verify before you install Copy Services Manager.

Prerequisites for IBM Z

Before you install Copy Services Manager, ensure that the hardware and software requirements are met.

Your system must meet the following prerequisites:

Hardware requirements

- Minimum disk space requirement: See the *IBM Copy Services Manager for z Systems Program Directory* or the *IBM Copy Services Manager Basic Edition for z Systems Program Directory* for details.
- Memory: 768 MB minimum memory allocation to UNIX System Services for Java™ virtual machine
- Processors: zIIP or zAAP processors should be used to handle the Copy Services Manager workload and avoid the cost of *millions of instructions per second* (MIPS). zIIP and zAAP are special processors that are used specifically for products that operate on WebSphere for z/OS and Java workloads.

Port requirements

Ensure that the ports that are shown in are available for use. The ports that are shown are the defaults. You can specify different ports if they are available for use.

Table 4. Server port requirements for IBM Z	
Port	**Default port number**
GUI	9559
CLI	9560
Active/Standby	9561

Software requirements

- Operating system: IBM z/OS
- z/OS versions: 2.1, 2.2, or 2.3

HyperSwap fixes and updates

To ensure that you have the most-recent z/OS APARs, updates, and program temporary fixes (PTFs) that are required to support HyperSwap, you can get the most-recent IBM HOLDDATA. When you have the HOLDDATA, you then use the fix category IBM.Function.HyperSwap to select and apply the appropriate PTFs or to identify any PTFs that are missing. For the most-recent information on HOLDDATA, see "Enhanced HOLDDATA for z/OS" at the support portal (http://service.software.ibm.com/holdata/390holddata.html). Use the full two-year file only. After you receive the most-recent HOLDDATA, you can use the SMP/E REPORT MISSINGFIX command to identify missing HyperSwap PTFs.

For more information about the REPORT MISSINGFIX command, see *SMP/E for z/OS Commands* document at http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss?CTY=US&FNC=SRX&PBL=SA22-7771-15.

Language considerations

If Copy Services Manager is installed on an operating system with a default locale that the product does not support, errors might occur during product operations.

Copy Services Manager supports the following language locales:

- Chinese - China (zh-CN)
- Czech (cs)
- French (fr)
- German (de)
- Hungarian (hu)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Polish (pl)
- Portuguese - Brazil (pt-BR)
- Russian (ru)
- Spanish (es)

Prerequisites for distributed systems

Before you install Copy Services Manager on distributed systems, ensure that the hardware and software requirements are met.

Disk space
   10 GB minimum

Memory
   1280 MB minimum

Processor
   Quad-core processor or higher recommended

Port requirements

   Ensure that the ports that are shown in are available for use. The ports that are shown are the defaults. You can specify different ports if they are available for use.

Table 5. Server port configuration for distributed systems	
Port	**Default port number**
GUI	9559
CLI	9560
Active/Standby	9561
Authentication	9562

Language considerations

If Copy Services Manager is installed on an operating system with a default locale that the product does not support, errors might occur during product operations.

Copy Services Manager supports the following language locales:

- Chinese - China (zh-CN)

- Czech (cs)
- French (fr)
- German (de)
- Hungarian (hu)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Polish (pl)
- Portuguese - Brazil (pt-BR)
- Russian (ru)
- Spanish (es)

Reconfiguring the management and authentication servers through bootstrap

You can modify the parameters of the bootstrap properties file to reconfigure the management and authentication servers.

1. Locate the bootstrap properties file for the server that is to be reconfigured.

   - For the management server, the bootstrap properties file is located at *installation_directory* `\liberty\wlp\usr\servers\csmServer\bootstrap.properties`.

   - For the authentication server, the bootstrap properties file is located at *installation_directory*`\liberty\wlp\usr\servers\csmAuth` `\bootstrap.properties`.

2. Modify one or more parameters.

   - If you choose to encrypt the keystore password, use the `securityUtility` password script located at *installation_directory*`/liberty/wlp/bin/`.

3. Restart the server.

Chapter 2. Installing Copy Services Manager

There are several steps to follow when you install Copy Services Manager. Certain prerequisites are also required, depending on whether you are installing on distributed systems, or IBM Z.

Installing on IBM Z

Follow these instructions to install Copy Services Manager on IBM Z.

To install Copy Services Manager, follow these steps:

1. Ensure that your system meets the minimum software and hardware requirements. See "Prerequisites for IBM Z" on page 1.

2. Verify that you have the latest z/OS APARs, updates, and PTFs needed to support Basic HyperSwap®. Use either the Technical help database for Mainframe Preventive Service Planning buckets website at http://www14.software.ibm.com/webapp/set2/psearch/search?domain=psp or the Enhanced PSP Tool or ServiceLink.

3. Install Copy Services Manager with SMP/E.

   a. Configure jobs

   b. Run jobs without errors

   For detailed installation instructions, see the *IBM Copy Services Manager for z Systems Program Directory* or the *IBM Copy Services Manager Basic Edition for z Systems Program Directory*. See "Publications and related information" on page viii for more details on where to find these directories.

4. Complete the postinstallation steps for z/OS.

   a. Configure the IWNRACF, IWNINSTL, and IWNSRV jobs. Optionally, you can also configure the IWNAUTH job. See "Configuring the IWNRACF jobs" on page 5, "Configuring the IWNINSTL job" on page 18, "Configuring the IWNSRV job" on page 21, and "Configuring the IWNAUTH job" on page 22 for more detailed information.

   b. Run the IWNINSTL installation job with no errors.

5. Start the Copy Services Manager graphical user interface (GUI) as described in "Installing on distributed systems" on page 23, step "11" on page 24.

Postinstallation tasks for IBM Z

After you install IBM Z, you must complete the postinstallation tasks. These tasks include configuring and submitting the jobs that are presented in the following topics in the order that they are presented.

Configuring the IWNRACF jobs

Starting with Copy Services Manager Version 6.2.5, you can complete five new postinstallation IWNRACF jobs: IWNRACF1, IWNRACF2, IWNRACF3, IWNRACF4, IWNRACF5 and (optional) IWNRACFC. These jobs provide the necessary security settings and write permissions for the file system, address spaces, user IDs, login authorities, and enablement of SAF authorization to run the Copy Services Manager application. You can find these jobs in the SYS1.SAMPLIB data set.

It can be useful to define several different user IDs when you install Copy Services Manager. These IDs are needed for the IBM Resource Access Control Facility (RACF®) security program on your target system.

Extra user IDs are required if you plan to install Copy Services Manager on z/OS to enable HyperSwap, or if you plan to use the HyperSwap Sockets Server, or both. To define these user IDs, you must run several IWNRACF jobs.

Note: You need to run the IWNRACF jobs after either the z/OS file system (zFS), or the hierarchical file system (HFS) is created, the mount job is run, and before you submit the IWNINSTL job. For more information, see "Configuring the IWNINSTL job" on page 18.

These IWNRACF jobs define the following items:

IWNRACF1 job
> Defines the Copy Services Manager default administrator and additional user IDs. The default admin ID is used for the IWNINSTL job *CSM_USER=#*`csm_user` variable. This default admin user is the one that can first be used to log in to the Copy Services Manager GUI or CLI. This user has administrative privileges, and can add access to other users defined in RACF that have an OMVS segment.

IWNRACF2 job
> Defines the user ID that is associated with the Copy Services Manager IWNSRV address space. This ID requires access to the OMVS production directory at *<path_prefix>*`/opt/IBM/CSM` as set in the IWNINSTL job.

IWNRACF3 job
> Defines the user IDs that are associated with the HyperSwap address spaces (HSIBAPI and HSIB). The user and group that are specified require access to OMVS when the HyperSwap Socket Server is being used.

IWNRACF4 job
> Defines the user IDs that are associated with the HyperSwap Sockets Server address space (BHIHSRV). This job is only necessary if you are going to manage HyperSwap from a system outside of the sysplex. For example from another z/OS sysplex, or from a distributed server.

IWNRACF5 job
> Defines the Copy Services Manager host connection ID.

(Optional)
> **IWNRACFC job**

> Enables SAF authorization based on access to a user-specified facility.

RACF group, OMVS GID, and OMVS UID assignment:

In general, RACF group names and OMVS group IDs (GIDs) need to be unique when they are associated with different user IDs (UIDs). Any authorities that are granted to the group are inherited by the users in that group. Groups can be shared when it is permitted for all of the user IDs in that group to have the same authorities that are granted to that group. For example, you might consider using the same group for the two HyperSwap address spaces, HSIBAPI (that is, IOSHSAPI) and HSIB (that is, IOSHMCTL), the HyperSwap Sockets Server address space (BHIHSRV), and the Copy Services Manager address space (IWNSRV). However, it is best to only grant access to ANT.REPLICATIONMANAGER to the user IDs for BHIHSRV and IWNSRV because the user IDs for HSIBAPI and HSIB do not require that authority.

The OMVS ID needs to be unique for all user IDs.

Configuring the IWNRACF job (deprecated)
You configure the IWNRACF job to provide the necessary security and write permissions for the file system to run the Copy Services Manager application. This job (now deprecated) is found in the `SYS1.SAMPLIB` data set.

Important: The following procedure corresponds to the original, single RACF job for Copy Services Manager installation, which is now being deprecated. If you are installing Copy Services Manager for the first time, run the IWNRACF jobs 1-5 as detailed in the sections later on. If you installed Copy Services Manager in the past and ran this single RACF job (IWNRACF), you do not need to run any of the new 1-5 RACF jobs.

Deprecated IWNRACF job procedure: Configure the following items for the IWNRACF job:

- User for Copy Services Manager
- User ID number
- Group ID number
- Home directory for the Copy Services Manager user
- Group for the Copy Services Manager ID

These items are needed for the RACF security program on your target system.

Use the following steps to configure, and then submit the IWNRACF job:

1. Locate the IWNRACF job in the SYS1.SAMPLIB data set and open it.
2. Modify the following procedure to meet the system requirements for the RACF security program in your environment. See the job header comments for the definition of the variables that are used in this job.

```
//IWNRACF    JOB <job parameters>
//*********************************************************************
//*  LICENSED MATERIALS - PROPERTY OF IBM                           *
//*  THIS PRODUCT CONTAINS "RESTRICTED MATERIALS OF IBM"            *
//*   (C) COPYRIGHT IBM CORPORATION 2007,2016.                      *
//*  ALL RIGHTS RESERVED.                                           *
//*                                                                 *
//*  IBM Copy Services Manager for z/OS                             *
//*                                                                 *
//*  CAUTION: This is neither a JCL procedure nor a complete job.   *
//*  Before using this job step, you will have to make the following *
//*  modifications:                                                 *
//*                                                                 *
//*   THIS JOB IS BEING DEPRECATED. NEW INSTALLS SHOULD UTILIZE     *
//*   THE NEW IWNRACF1-5 JOBS, AS APPROPRIATE TO YOUR ENVIRONMENT.  *
//*                                                                 *
//*  1) Change the job card to meet your system requirements.       *
//*  2) Replace the following variables:                            *
//*          #csm_id  - User for CSM                                *
//*          #csm_grp - Group for the CSM id to belong to           *
//*          #gid     - Group id number                             *
//*          #uid     - User id number                              *
//*          #ussPath - Home directory for #csm_id                  *
//*                                                                 *
//*********************************************************************
/*
//ANTRAC  EXEC PGM=IKJEFT01
//SYSLBC   DD DSN=SYS1.BRODCAST,DISP=SHR
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
  /* Define CSM user and group */
  ADDGROUP #csm_grp OMVS(GID(#gid))
  ADDUSER #csm_id DFLTGRP(#csm_grp) OMVS(UID(#uid) +
     HOME(#ussPath) +
     PROGRAM(/bin/sh)) NAME('Liberty') NOPASSWORD NOOIDCARD
  ALU #csm_id PASSWORD(#csm_id) NOEXPIRE

  /* Define Started profiles */
  RDEF STARTED IWNSRV.* UACC(NONE) STDATA(USER(#csm_id) +
     GROUP(#csm_grp) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
  SETROPTS RACLIST(STARTED) GENERIC(STARTED) REFRESH

  /* Define ANT.REPLICATIONMANAGER */
  RDEFINE FACILITY ANT.REPLICATIONMANAGER UACC(NONE)
  PERMIT ANT.REPLICATIONMANAGER CLASS(FACILITY) +
     ID(#csm_id) ACCESS(CONTROL)
  SETROPTS RACLIST(FACILITY) REFRESH
/*
```

3. After you replace the variables, submit the IWNRACF job.

Configuring the IWNRACF1 job: Copy Services Manager default administrator and additional IDs
The IWNRACF1 job defines the Copy Services Manager default administrator and additional user IDs.

The IWNRACF1 job must be run at least one time when Copy Services Manager is installed on z/OS. This job creates the default Copy Services Manager administrator user ID that is used to log in to the Copy Services Manager GUI.

Note: It is suggested that you use *CSMUSER* as the default Copy Services Manager administrator user ID. This default user ID must also be specified in the **#csm_user** parameter in the IWNINSTL job. For more information, see

You can run this job again if you want to have more than one user ID to log in to Copy Services Manager. Having multiple Copy Services Manager user IDs provides an audit trail to identify who issues replication commands. With multiple user IDs, you can also customize the restrictions that are placed on each user.

The auditing capabilities on the z/OS HyperSwap side are limited because HyperSwap only authenticates the Copy Services Manager server that is connecting to it. However, Copy Services Manager provides auditing at the command level.

User IDs are required to log in to the Copy Services Manager server through the GUI. Three different user roles can be associated with a Copy Services Manager login ID: monitor, operator, or administrator.

If you do not install the Copy Services Manager server on a z/OS platform, then this job is not necessary, even if the Copy Services Manager server is connected to HyperSwap over the Sockets Server. The HyperSwap function does not receive or require information about each Copy Services Manager login ID. HyperSwap only authenticates to the Copy Services Manager server that is connecting to it. The Copy Services Manager installation ensures that only commands that are authorized to each Copy Services Manager user are forwarded to HyperSwap for processing.

Each Copy Services Manager user ID needs to have the following attributes:

- No Time Sharing Option (TSO) segment. No one should ever log in to TSO with this user ID.
- An associated password.
- An OMVS segment with both a valid OMVS ID and OMVS GID. This segment is required for the user ID to be located and displayed on the **Add User** page.

Use the following steps to configure, and then submit the IWNRACF1 job:

1. Locate the IWNRACF1 job in the SYS1.SAMPLIB data set and open it.
2. Modify the following procedure to meet the system requirements for the RACF security program in your environment. See the job header comments for the definition of the variables that are used in this job.

```
//IWNRACF1   JOB <job parameters>
//********************************************************************
//*  LICENSED MATERIALS - PROPERTY OF IBM                           *
//*  THIS PRODUCT CONTAINS "RESTRICTED MATERIALS OF IBM"            *
//*   (C) COPYRIGHT IBM CORPORATION 1999, 2016.                     *
//*  ALL RIGHTS RESERVED.                                           *
//*                                                                 *
//*  Copy Services Manager for z Systems                            *
//*                                                                 *
//*  CAUTION: This is neither a JCL procedure nor a complete job.   *
//*  Before you use this job step, make the following modifications:*
//*                                                                 *
//*  This job defines the user IDs that are associated with the     *
//*  default Copy Services Manager login ID, and can                *
//*  be used to create additional Copy Services Manager login IDs.  *
//*                                                                 *
//*                                                                 *
//*  1) Change the job card to meet your system requirements.       *
//*  2) Replace the following variables:                            *
//*        #csm_user - User ID that is used for the Copy Services   *
//*                    Manager login.                               *
//*                  - It is suggested that you use "CSMUSER"       *
//*                    as the default Copy Services Manager         *
//*                    administrator user ID.                       *
//*                  - Set the CSM_USER parameter in the IWNINSTL   *
//*                    job to the default Copy Services Manager     *
//*                    administrator ID that is specified here.     *
//*                  - Subsequent users can be created and added    *
//*                    by using this job.                           *
//*        #group_name - Group name for Copy Services Manager.      *
//*                  - Set the CSM_GRP parameter in the IWNINSTL    *
//*                    job to the group name that is specified      *
//*                    here.                                        *
//*        #csm_pw   - Initial password for Copy Services Manager.  *
//*        #gid      - Group ID number.                             *
//*        #uid      - User ID number.                              *
//*        #ussPath  - Home directory for #csm_user, for example    *
//*                    <-path_prefix>/opt/IBM/CSM                   *
//*                    as set in the IWNINSTL job.                   *
//*        #interval - The number of days before the password must  *
//*                    be changed. Specify NOINTERVAL if you        *
//*                    never want the password to expire.           *
//*                                                                 *
//********************************************************************
/*
```

```
//CSMLOGON EXEC PGM=IKJEFT01
//SYSLBC   DD DSN=SYS1.BRODCAST,DISP=SHR
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
  /* Define Copy Services Manager login user ID                    */
  ADDGROUP #group_name OMVS(GID(#gid))
  ADDUSER #csm_user DFLTGRP(#group_name) OMVS(UID(#uid) +
      HOME(#ussPath) +
      PROGRAM(/bin/sh)) +
      NAME('Copy Services Manager User ID')
  ALU #csm_user PASSWORD(#csm_pw) NOEXPIRED
  PASSWORD INTERVAL(#interval) USER(#csm_user)
/*
```

3. After you replace the variables, submit the IWNRACF1 job.

Configuring the IWNRACF2 job: Copy Services Manager address space

The IWNRACF2 job specifies the user ID that is associated with the Copy Services Manager address space (IWNSRV).

The IWNRACF2 job must be run at least one time when Copy Services Manager is installed on z/OS. The IWNSRV user ID is associated with the Copy Services Manager address spaces (IWNSRV and IWNAUTH) and needs to have the following attributes:

- No TSO segment. No one should ever log in to TSO with this user ID.

- Be given the PROTECTED attribute by specifying the NOPASSWORD keyword. The PROTECTED attribute means that the password cannot be revoked because no password exists. Therefore, it is protected from someone who attempts to get the user ID revoked by repeated failed password attempts.

- Authorized to the ANT.REPLICATIONMANGER RACF Facility because this user ID is used by the HyperSwap Java Native Interface (JNI) to authenticate Copy Services Manager.

- An OMVS segment with both a valid OMVS ID and OMVS GID because the Copy Services Manager address space uses z/OS UNIX System Services (USS).

- Specified in the **CSM_ADDR_OWNER** parameter in the IWNINSTL job. For more information, see

Use the following steps to configure, and then submit the IWNRACF2 job:

1. Locate the IWNRACF2 job in the SYS1.SAMPLIB data set and open it.

2. Modify the following procedure to meet the system requirements for the RACF security program in your environment. See the job header comments for the definition of the variables that are used in this job.

```
//IWNRACF2  JOB <job parameters>
//********************************************************************
//*  LICENSED MATERIALS - PROPERTY OF IBM                           *
//*  THIS PRODUCT CONTAINS "RESTRICTED MATERIALS OF IBM"            *
//*   (C) COPYRIGHT IBM CORPORATION 1999, 2016.                     *
//*  ALL RIGHTS RESERVED.                                           *
//*                                                                 *
//*  IBM Copy Services Manager for z/OS                             *
//*                                                                 *
//*  CAUTION: This is neither a JCL procedure nor a complete job.   *
//*  Before you use this job step, make the following modifications: *
//*                                                                 *
//*  This job defines the user IDs that are associated with the     *
//*  Copy Services Manager address spaces - IWNSRV and              *
//*  optionally IWNAUTH.                                            *
//*                                                                 *
//*  1) Change the job card to meet your system requirements.       *
//*  2) Replace the following variables:                            *
//*          #user_id  - User ID for the Copy Services Manager      *
//*                      started tasks.                             *
//*                    - It is suggested that you use "IWNSRV"      *
//*                      as the user ID.                            *
//*          #group_name - Group name for the IWNSRV and            *
//*                      optional IWNAUTH                           *
//*                      address spaces.                            *
//*          #gid      - Group ID number for the IWNSRV and         *
//*                      optional IWNAUTH                           *
//*                      address spaces.                            *
//*          #uid      - User ID number.                            *
```

```
//*          #ussPath  - Home directory for #user_id, for example   *
//*                     <-path_prefix>/opt/IBM/CSM               *
//*                     as set in the IWNINSTL job.              *
//*                                                              *
//******************************************************************
/*
//IWNSRV    EXEC PGM=IKJEFT01
//SYSLBC    DD DSN=SYS1.BRODCAST,DISP=SHR
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
  /* Define the Copy Services Manager address space user ID.        */
  ADDGROUP #group_name OMVS(GID(#gid))
  ADDUSER #user_id DFLTGRP(#group_name) OMVS(UID(#uid) +
       HOME(#ussPath) +
       PROGRAM(/bin/sh)) +
       NAME('Copy Services Manager Address Spaces') +
       NOPASSWORD

  /* Define the started profiles.                                   */
  RDEF STARTED IWNSRV.* UACC(NONE) STDATA(USER(#user_id) +
       GROUP(#group_name) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
  RDEF STARTED IWNAUTH.* UACC(NONE) STDATA(USER(#user_id) +
       GROUP(#group_name) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))

  /* If you plan on utilizing LDAP on the system uncomment the      */
  /*   following lines
  RDEF STARTED IWNAUTH.* UACC(NONE) STDATA(USER(#user_id) +
       GROUP(#group_name) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))

  SETROPTS RACLIST(STARTED) GENERIC(STARTED) REFRESH

  /* Permit access to ANT.REPLICATIONMANAGER.                       */
  RDEFINE FACILITY ANT.REPLICATIONMANAGER UACC(NONE)
  PERMIT ANT.REPLICATIONMANAGER CLASS(FACILITY) +
       ID(#user_id) ACCESS(CONTROL)

  /* If the user is running a Liberty Angel server uncomment     */
  /* the following 2 lines                                       */
  /* RDEF SERVER BBG.ANGEL UACC(NONE)                            */
  /* PERMIT BBG.ANGEL CLASS(SERVER) ACCESS(READ) ID(#user_id)    */

  SETROPTS RACLIST(FACILITY) REFRESH
  /*
```

3. After you replace the variables, submit the IWNRACF2 job.

Configuring the IWNRACF3 job: HyperSwap address spaces

The IWNRACF3 job defines the user ID that is associated with the HyperSwap address spaces.

You need to define user IDs for the two HyperSwap address spaces. The two HyperSwap address spaces are HyperSwap API address space (HSIBAPI), and HyperSwap management address space (HSIB).

Note: When you run the IWNRACF3 and IWNRACF4 jobs, it might be useful to consult the section titled *Securing communication between z/OS HyperSwap and the CSM Server* in the IBM Redbooks publication *IBM Copy Services Manager Implementation Guide* (http://www.redbooks.ibm.com/abstracts/sg248375.html).

You need to run this job in the following situations:

- If Copy Services Manager is used to manage a session with the z/OS HyperSwap function, or Metro Mirror with the Hardened Freeze option.
- Any time that Copy Services Manager connects to z/OS through the HyperSwap Sockets Server.

Even if no sessions are enabled for either HyperSwap or Hardened Freeze, the HyperSwap address spaces allow channel command words (CCWs) to be issued.

The user IDs associated with the two HyperSwap address spaces (HSIBAPI and HSIB) need to have the following attributes:

- No TSO segment. No one should ever log in to TSO with this user ID.
- Be given the PROTECTED attribute by specifying the NOPASSWORD keyword. The PROTECTED attribute means that the password cannot be revoked because no password exists. Therefore, it is protected from someone who attempts to get the user ID revoked by repeated failed password attempts.

- An OMVS segment with both a valid OMVS ID and OMVS GID because the HyperSwap address spaces use z/OS UNIX System Services (USS). Technically, you do not need the OMVS segment if you do not specify the **SOCKPORT** parameter on the EXEC card for HSIB (IOSHMCTL). However, it is best to define the OMVS segment now in case you later decide to use the HyperSwap Sockets Server.

Notes: It is suggested that you use HSIBAPI and HSIB for the HyperSwap started tasks. When you define the **STARTED** class, you must specify the member name.

- Some customers place the started task for the HyperSwap management address space in SYS1.PROCLIB as IOSHMCTL. In that case, either you must rename the member of SYS1.PROCLIB to HSIB, or the JCL must specify "RDEF STARTED IOSHMCTL.*" instead.

- Some customers place the started task for the HyperSwap API address space in SYS1.PROCLIB as IOSHSAPI. In that case, either you must rename the member of SYS1.PROCLIB to HSIBAPI, or the JCL must specify "RDEF STARTED IOSHSAPI.*" instead.

Use the following steps to configure, and then submit the IWNRACF3 job:

1. Locate the IWNRACF3 job in the SYS1.SAMPLIB data set and open it.
2. Modify the following procedure to meet the system requirements for the RACF security program in your environment. See the job header comments for the definition of the variables that are used in this job.

```
//IWNRACF3   JOB <job parameters>
//*********************************************************************
//*  LICENSED MATERIALS - PROPERTY OF IBM                           *
//*  THIS PRODUCT CONTAINS "RESTRICTED MATERIALS OF IBM"            *
//*   (C) COPYRIGHT IBM CORPORATION 1999, 2016.                     *
//*  ALL RIGHTS RESERVED.                                           *
//*                                                                 *
//*  IBM Copy Services Manager for z/OS                             *
//*                                                                 *
//*  CAUTION: This is neither a JCL procedure nor a complete job.   *
//*  Before you use this job step, make the following modifications: *
//*                                                                 *
//*  This job defines the user IDs that are associated with the two *
//*  HyperSwap address spaces:                                      *
//*  - HyperSwap API address space - HSIBAPI                        *
//*  - HyperSwap Management address space - HSIB                    *
//*                                                                 *
//*                                                                 *
//*  1) Change the job card to meet your system requirements.       *
//*  2) Replace the following variables:                            *
//*          #user_id  - User ID for the HyperSwap address spaces.  *
//*                    - It is suggested that you use "HSIB" as the *
//*                      user ID.                                   *
//*          #group_name - Group name for the HyperSwap address     *
//*                      spaces.                                     *
//*          #gid      - Group ID number.                           *
//*          #uid      - User ID number.                            *
//*********************************************************************
/*
//HSIB      EXEC PGM=IKJEFT01
//SYSLBC    DD DSN=SYS1.BRODCAST,DISP=SHR
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
  /* Define the HyperSwap address space user ID and group.        */
  ADDGROUP #group_name OMVS(GID(#gid))
  ADDUSER #user_id DFLTGRP(#group_name) OMVS(UID(#uid) +
      HOME('/')) +
      NAME('HyperSwap Address Spaces') +
      NOPASSWORD

  /* Define the started profiles.                                 */
  RDEF STARTED HSIBAPI.* UACC(NONE) STDATA(USER(#user_id)     +
      GROUP(#group_name) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
  RDEF STARTED HSIB.* UACC(NONE) STDATA(USER(#user_id)      +
      GROUP(#group_name) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
  SETROPTS RACLIST(STARTED) GENERIC(STARTED) REFRESH
/*
```

3. After you replace the variables, submit the IWNRACF3 job.

Configuring the IWNRACF4 job: HyperSwap Sockets Server address space
The IWNRACF4 job defines the user ID associated with the HyperSwap Sockets Server address space (BHIHSRV).

You only need to run this job if Copy Services Manager connects to z/OS by using the HyperSwap Sockets Server.

The user ID associated with the HyperSwap Sockets Server address space (BHIHSRV) needs to have the following attributes:

- No TSO segment. No one should ever log in to TSO with this user ID.
- Be given the PROTECTED attribute by specifying the NOPASSWORD keyword. The PROTECTED attribute means that the password cannot be revoked because no password exists. Therefore, it is protected from someone who attempts to get the user ID revoked by repeated failed password attempts.
- Authorized to the ANT.REPLICATIONMANGER RACF Facility. You might need to create (RDEFINE) the ANT.REPLICATIONMANGER RACF Facility if Copy Services Manager is not installed on z/OS, and you have not already run the IWNRACF2 job.
- An OMVS segment with both a valid OMVS ID and OMVS GID because the HyperSwap Sockets Server uses z/OS UNIX System Services (USS).

Note: When you run the IWNRACF3 and IWNRACF4 jobs, it might be useful to consult the section titled *Securing communication between z/OS HyperSwap and the CSM Server* in the IBM Redbooks publication *IBM Copy Services Manager Implementation Guide* (http://www.redbooks.ibm.com/abstracts/sg248375.html).

Use the following steps to configure, and then submit the IWNRACF4 job:

1. Locate the IWNRACF4 job in the SYS1.SAMPLIB data set and open it.
2. Modify the following procedure to meet the system requirements for the RACF security program in your environment. See the job header comments for the definition of the variables that are used in this job.

```
//IWNRACF4   JOB <job parameters>
//********************************************************************
//*  LICENSED MATERIALS - PROPERTY OF IBM                           *
//*  THIS PRODUCT CONTAINS "RESTRICTED MATERIALS OF IBM"            *
//*   (C) COPYRIGHT IBM CORPORATION 1999, 2016.                     *
//*  ALL RIGHTS RESERVED.                                           *
//*                                                                 *
//*  IBM Copy Services Manager for z/OS                             *
//*                                                                 *
//*  CAUTION: This is neither a JCL procedure nor a complete job.   *
//*  Before you use this job step, make the following modifications: *
//*                                                                 *
//*  This job defines the user ID that is associated with the       *
//*  HyperSwap Sockets Server address space - BHIHSRV.              *
//*                                                                 *
//*                                                                 *
//*  1) Change the job card to meet your system requirements.       *
//*  2) Replace the following variables:                            *
//*         #user_id  - User ID for the HyperSwap Sockets Server    *
//*                     address space.                              *
//*                     - It is suggested that you use "BHIHSRV"    *
//*                       as the user ID.                           *
//*         #group_name - Group name for the HyperSwap address      *
//*                     space.                                      *
//*         #gid      - Group ID number.                            *
//*         #uid      - User ID number.                             *
//*                                                                 *
//********************************************************************
/*
//BHIHSRV  EXEC PGM=IKJEFT01
//SYSLBC   DD DSN=SYS1.BROADCAST,DISP=SHR
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
   /* Define the HyperSwap Sockets Server address space            */
   /* user ID and group.                                           */
   ADDGROUP #group_name OMVS(GID(#gid))
   ADDUSER #user_id DFLTGRP(#group_name) OMVS(UID(#uid)  +
      HOME('/') +
```

```
        PROGRAM(/bin/sh)) +
        NAME('HyperSwap Sockets Server') +
        NOPASSWORD

    /* Define the started profile.                              */
    RDEF STARTED BHIHSRV.* UACC(NONE) STDATA(USER(#user_id) +
        GROUP(#group_name) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
    SETROPTS RACLIST(STARTED) GENERIC(STARTED) REFRESH

    /* Permit access to ANT.REPLICATIONMANAGER.                 */
    RDEFINE FACILITY ANT.REPLICATIONMANAGER UACC(NONE)
    PERMIT ANT.REPLICATIONMANAGER CLASS(FACILITY) +
        ID(#user_id) ACCESS(CONTROL)
    SETROPTS RACLIST(FACILITY) REFRESH
/*
```

3. After you replace the variables, submit the IWNRACF4 job.

Configuring the IWNRACF5 job: Copy Services Manager z/OS host connection ID

The IWNRACF5 job defines the user ID associated with the Copy Services Manager z/OS host connection ID. This user ID is used to authenticate Copy Services Manager to the HyperSwap Sockets Server.

If you manage multiple sysplexes from one or more instances of Copy Services Manager, you might choose to have a single host connection ID for all Copy Services Manager to HyperSwap connections. However, you might choose to have different host connection IDs for each sysplex to the Copy Services Manager instance.

The Copy Services Manager active and standby servers use the same host connection IDs.

Note: The user ID specified on the sockets connection is used to authenticate a valid instance of Copy Services Manager that is attempting to connect to HyperSwap. However, it does not identify the specific user that is using the Copy Services Manager GUI. The three user roles in Copy Services Manager are monitor, operator, or administrator. HyperSwap does not enforce user roles, only Copy Services Manager enforces them.

The Copy Services Manager host connection ID needs to have the following attributes:

- No TSO segment. No one should ever log in to TSO with this user ID.
- An associated password.
- Authorized to the ANT.REPLICATIONMANGER RACF Facility. You might need to create (RDEFINE) the ANT.REPLICATIONMANGER RACF Facility if Copy Services Manager is not installed on z/OS, and you have not already run the IWNRACF2 job.

Use the following steps to configure, and then submit the IWNRACF5 job:

1. Locate the IWNRACF5 job in the SYS1.SAMPLIB data set and open it.
2. Modify the following procedure to meet the system requirements for the RACF security program in your environment. See the job header comments for the definition of the variables that are used in this job.

```
//IWNRACF5   JOB <job parameters>
//*****************************************************************
//*  LICENSED MATERIALS - PROPERTY OF IBM                        *
//*  THIS PRODUCT CONTAINS "RESTRICTED MATERIALS OF IBM"         *
//*   (C) COPYRIGHT IBM CORPORATION 1999, 2016.                  *
//*  ALL RIGHTS RESERVED.                                        *
//*                                                              *
//*  IBM Copy Services Manager for z/OS                          *
//*                                                              *
//*  CAUTION: This is neither a JCL procedure nor a complete job.*
//*  Before you use this job step, make the following modifications:*
//*                                                              *
//*  This job defines the user ID that can be used to authenticate *
//*  the Copy Services Manager to the HyperSwap Sockets Server.  *
//*                                                              *
//*                                                              *
//*  1) Change the job card to meet your system requirements.    *
//*  2) Replace the following variables:                         *
//*        #user_id  - User ID that is used for the Copy Services *
//*                    Manager host connection.                  *
//*                  - Additional Copy Services Manager host     *
```

```
//*                      connection user IDs can be created and       *
//*                      added by using this job.                     *
//*          #group_name - Group name for the Copy Services Manager   *
//*                      host connection user ID.                     *
//*          #csm_pw   - Initial password for the Copy Services       *
//*                      Manager host connection user ID.             *
//*          #interval - The number of days before the password must *
//*                      be changed. Specify NOINTERVAL if you        *
//*                      never want the password to expire.           *
//*                                                                    *
//*********************************************************************
/*
//CSMHOST  EXEC PGM=IKJEFT01
//SYSLBC   DD DSN=SYS1.BROADCAST,DISP=SHR
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
  /* Define the Copy Services Manager host connection user.          */
  ADDGROUP #group_name
  ADDUSER #user_id DFLTGRP(#group_name) +
     NAME('Copy Services Manager Host Connection User ID')
  ALU #user_id PASSWORD(#csm_pw) NOEXPIRED
  PASSWORD INTERVAL(#interval) USER(#user_id)

  /* Permit access to ANT.REPLICATIONMANAGER.                        */
  RDEFINE FACILITY ANT.REPLICATIONMANAGER UACC(NONE)
  PERMIT ANT.REPLICATIONMANAGER CLASS(FACILITY) +
     ID(#user_id) ACCESS(CONTROL)
  SETROPTS RACLIST(FACILITY) REFRESH
/*
```

3. After you replace the variables, submit the IWNRACF5 job.

Configuring the IWNRACFC job: Copy Services Manager enable SAF authorization based on access to a user-specified facility

The optional IWNRACFC job creates or updates a user's authority to access a z/OS System Authorization Facility (SAF). With access to a SAF, a user can authenticate and access the CLI, without the need to provide a password.

The additional permissions with SAF ensure that users already have access to the OMVS system. If the users have OMVS system access, it means that they have already logged in and authenticated to the OMVS system.

This optional job also defines the new facility that a customer can use, or customize to the facility of their choosing. The user also needs to be granted access to the BPX.DAEMON and BPX.SERVER FACILITY classes for the native SAF calls from the CLI and IWNSRV. Access to these classes ensures that the user has authorization to the given facility. For this job, the CLI and Copy Services Manager GUI server must be running on the same sysplex, and have access to same RACF instance.

Use the following steps to configure, and then submit the IWNRACFC job:

1. Locate the IWNRACFC job in the SYS1.SAMPLIB data set and open it.
2. Modify the following procedure to meet the system requirements for the RACF security program in your environment. See the job header comments for the definition of the variables that are used in this job.

```
//IWNRACFC    JOB <job parameters>
//*********************************************************************
//*  LICENSED MATERIALS - PROPERTY OF IBM                          *
//*  THIS PRODUCT CONTAINS "RESTRICTED MATERIALS OF IBM"           *
//*   (C) COPYRIGHT IBM CORPORATION 2007,2019.                     *
//*  ALL RIGHTS RESERVED.                                          *
//*                                                                *
//*  IBM Copy Services Manager for z/OS                            *
//*                                                                *
//*  CAUTION: This is neither a JCL procedure nor a complete job.  *
//*  Before using this job step, make the following               *
//*  modifications:                                                *
//*                                                                *
//*  This job creates a user in RACF and places the user into a    *
//*  facility class that is authorized to access the CLI  and      *
//*  initiate scripts without the need for credential prompts.     *
//*  The user is validated against the specified facility and      *
//*  is required to have read access. If access is revoked, the user *
//*  is not allowed to access the CLI. This user must also be      *
```

```
//*  added through the Administration panel with a valid user role.   *
//*  The default facility that is defined in this class is used unless*
//*  a different one is specified in the repcli.properties file as     *
//*  facility=IWNSRV.CLIAUTH.                                          *
//*                                                                    *
//*  The following requirements for using this feature include:       *
//* 1) The CLI and Copy services manager GUI server must reside        *
//*    on the same system.                                            *
//* 2) You must be logged in as a TSO user when running the command.  *
//* 3) The TSO user that you are logged in as must be added to        *
//*    Copy Services Manager.                                         *
//* 4) LDAP must be disabled through the IWNINSTL job, as follows:     *
//*     ENABLE_LDAP=FALSE, which is the default.                      *
//*     If Copy Services Manager is already installed, IWNINSTL must  *
//*     be re-run to disable LDAP.                                    *
//* 5) This feature is restricted to being used by one user unless    *
//*    write permission is given to the cliTrace.log file for other  *
//*    users in the group.                                           *
//* 6) This job must be tailored to your environment and used as a    *
//*    guideline for permissions that are required for the           *
//*    function to work.                                             *
//* 7) The following commands must be run under OMVS before you       *
//*    attempt to run a command using the SAF switch:                *
//*    - Give program control to the Java executable under           *
//*      Copy Services Manager:                                      *
//*          extattr +p /opt/IBM/CSM/Java/bin/java                   *
//*    - Give the following authority for the CLI folders and the    *
//*      users home directory:                                       *
//*          chmod 775 /opt/IBM/CSM                                  *
//*          chmod 775 /opt/IBM/CSM/CLI                             *
//*          chmod 775 /opt/IBM/CSM/CLI/cliTrace.log               *
//*          chmod 760 #ussPath/.sh_history                        *
//*                                                                    *
//* 8) To enable the new login module, you must update the           *
//*    configuration file csm.conf as shown:                        *
//*    The configuration file is located in the                     *
//*    <CSM_ProductionRoot>/wlp/usr/servers/csmServer/properties/   *
//*    directory, and must be replaced and updated with             *
//*    the following information:                                   *
//*    (OEDIT under TSO or upload using FTP in EBCDIC)              *
//*                                                                    *
//* CSMServer {                                                      *
//*  com.ibm.csm.server.security.CertificateLoginModule SUFFICIENT;  *
//*  com.ibm.csm.server.security.SAFLoginModule SUFFICIENT;         *
//*  com.ibm.csm.server.security.WebSphereLoginModule SUFFICIENT;   *
//*  };                                                             *
//*                                                                    *
//* 9) The <CSM_ProductionRoot>/CLI/repcli.properties file requires  *
//*    the following lines to be added:                             *
//*    (OEDIT under TSO or upload using FTP in EBCDIC)              *
//*    useSAF=true                                                  *
//*    FACILITY=IWNSRV.CLIAUTH                                      *
//*                                                                    *
//*  Note: The new optional parameter -saf can be used on the command *
//*    line if you do not want to include it in the above file.      *
//*    (See the CLI Guide for examples of using the parameter with a  *
//*    command.)                                                     *
//*                                                                    *
//*  10) Restart the IWNSRV job and ensure that the TSO user has been *
//*      added.                                                      *
//*                                                                    *
//*  Steps to complete this job:                                     *
//* 1) Change the job card to meet your system requirements.         *
//* 2) Replace the following variables:                             *
//*          #csm_id  - User for auto login                         *
//*          #csm_pw  - Password for auto login                     *
//*          #csm_grp - Group for the user as defined in IWNRACF1    *
//*          #gid      - Group id number                            *
//*          #uid     - User id number                              *
//*          #ussPath  - Home directory for #csm_id                 *
//*          IWNSRV.CLIAUTH - Facility to authorize access for user  *
//*                     as defined in repcli.properties on USS       *
//*          #srvr_id  - Owner of IWNSRV created by IWNRACF2         *
//*                                                                    *
//********************************************************************
/*
//IWNRACFC  EXEC PGM=IKJEFT01
//SYSLBC    DD DSN=SYS1.BRODCAST,DISP=SHR
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
  /* Define CSM SAF user and group (if not already defined).      */
  ADDGROUP #csm_grp OMVS(GID(#gid))
```

```
        ADDUSER #csm_id DFLTGRP(#csm_grp) OMVS(UID(#uid) +
            HOME(#ussPath) +
            PROGRAM(/bin/sh)) NAME('CSM SAF USER')
        ALU #csm_id PASSWORD(#csm_pw) NOEXPIRE

        /* Define the IWNSRV.CLIAUTH facility. */
        RDEFINE FACILITY IWNSRV.CLIAUTH UACC(NONE)
        PERMIT IWNSRV.CLIAUTH CLASS(FACILITY) +
            ID(#csm_id) ACCESS(READ)

        /* The SAF native calls require that the user who is logged in to */
        /* OMVS and the IWNSRV owner be granted access to                 */
        /* BPX.SERVER and BPX.DAEMON.                                     */
        RDEFINE FACILITY BPX.SERVER UACC(NONE) OWNER(SYS1)
        PERMIT BPX.DAEMON CLASS(FACILITY) ID(#csm_id) ACCESS(NONE)
        PERMIT BPX.SERVER CLASS(FACILITY) ID(#csm_id) ACCESS(READ)
        PERMIT BPX.SERVER CLASS(FACILITY) ID(#srvr_id) ACCESS(READ)

        SETROPTS RACLIST(FACILITY) REFRESH
   /*
```

3. After you replace the variables, submit the IWNRACFC job.

4. Run the following commands under OMVS before you attempt to run a command using the SAF switch:

   a) Give program control to the Java executable under Copy Services Manager:
   ```
   extattr +p /opt/IBM/CSM/Java/bin/java
   ```

   b) Give the following authority for the CLI folders and the user's home directory:
   ```
   chmod 775 /opt/IBM/CSM
   chmod 775 /opt/IBM/CSM/CLI
   chmod 775 /opt/IBM/CSM/CLI/cliTrace.log
   chmod 760 #ussPath/.sh_history
   ```

5. To enable the new login module, you must update the configuration file, `csm.conf`, as shown. You can use OEDIT under TSO, or upload using FTP in EBCDIC. The configuration file is located in the *<CSM_ProductionRoot>*/wlp/usr/servers/csmServer/properties directory, and must be replaced and updated with the following information:

   Note: The default of the first line in the file is **CSMDisabled**, which you need to replace with **CSMServer**. Also add the entry as shown in **bold**.

   ```
   CSMServer {
   com.ibm.csm.server.security.CertificateLoginModule SUFFICIENT;
   com.ibm.csm.server.security.SAFLoginModule SUFFICIENT;
   com.ibm.csm.server.security.WebSphereLoginModule SUFFICIENT;
   };
   ```

6. Edit the *<CSM_ProductionRoot>*/CLI/repcli.properties file by adding the following lines:
   ```
   useSAF=true
   FACILITY=IWNSRV.CLIAUTH
   ```

   Notes:

   - If you want to specify a facility other than the default, you must specify the following property in the `repcli.properties` file: FACILITY=IWNSRV.CLIAUTH. Otherwise the default facility ANT.REPLICATIONMANAGER is used.

   - The new optional parameter **-saf** can be used on the command line if you do not want to include it in the `repcli.properties` file. See the *Copy Services Manager Command-Line Interface User's Guide* for more information on using the **saf** command parameter. You can find details on where to obtain this guide in "Publications and related information" on page viii.

7. Restart the IWNSRV job.

8. Add the newly created user to Copy Services Manager through the **Settings** > **Administration** panel in the GUI, or by using the **mkuser** command at the CLI.

Migrating the file system from HFS to zFS

You can migrate from the hierarchical file system (HFS) to the z/OS file system (zFS).

The recommended file system to use is zFS. The zFS displays improved performance characteristics over HFS, and is the strategic direction for z/OS file systems.

Note: While it is recommended that you migrate from HFS to zFS, it is not currently a requirement.

Go to https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.2.0/com.ibm.zos.v2r2.bpxb200/hfszfsmi.htm for detailed information on how to migrate from HFS to zFS.

Configuring the IWNCRZFS job

You allocate a z/OS (zFS) data set to a root file system by specifying certain parameters in the IWNCRZFS job.

The files within a zFS data set are identified by their path and file names within Copy Services Manager.

1. Locate the IWNCRZFS job in the SYS1.SAMPLIB data set and open it.
2. Modify the following values on your system.

   Note: You can use either a z/OS file system (zFS) or hierarchical file system (HFS). However, the following sample job pertains only to those customers who are using a zFS. It is recommended that you use zFS.

```
//****************************************************************
//CREATZFS EXEC PGM=IDCAMS,REGION=64M
//SYSPRINT DD SYSOUT=A
//SYSIN    DD   *
   DEFINE                               +
     CLUSTER                            +
       (NAME('#CSM.ZFS')                +
       LINEAR                           +
TRK(50000,5000)                         +
       VOLUME(#VOLUME)                  +
SHAREOPTIONS(3))
/*
//* Format zFS - Note lowercase below for PARM in FORMTZFS
//FORMTZFS EXEC PGM=IOEAGFMT,REGION=64M,
//  PARM='-aggregate #CSM.ZFS -compat'
//SYSPRINT DD   SYSOUT=A
//STDOUT   DD   SYSOUT=A
/*
```

3. Specify the zFS to be created by editing the **NAME** (*#CSM.ZFS*) parameter.
4. The **TRK** parameter is already defined with the default data set size of *(50000, 5000)*.
5. Specify the **VOLUME** parameter; enter the volume name where the *zFS* resides. The default name of the volume is *(#VOLUME)*.
6. Submit the IWNCRZFS job.

Configuring the IWNCRHFS job

You allocate a hierarchical file system (HFS) data set to a root file system by specifying certain parameters in the IWNCRHFS job.

The files within an HFS data set are identified by their path and file names within Copy Services Manager.

1. Locate the IWNCRHFS job in the SYS1.SAMPLIB data set and open it.
2. Modify the following values on your system.

   Note: You can use either an HFS or z/OS file system (zFS). However, the following sample job pertains only to those customers who are using an HFS.

```
//****************************************************************
//CREATHFS EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
   PROFILE WTPMSG MSGID
   TIME

   ALLOC F(X) DA('#CSM.HFS') NEW CATALOG +
```

```
                DSNTYPE(HFS) +
                SPACE(50000,5000) TRACKS DIR(1) +
                VOL(#VOLUME)
   /*
```

3. Specify the HFS to be created by editing the **DA** (*#CSM.HFS*) parameter.
4. Specify the **DSNTYPE** parameter; enter *HFS* for z/OS system users.

   The **SPACE** parameter is already defined with the default data set size of *(50000, 5000)*.
5. Specify the **VOL** parameter; enter the volume name where the *HFS* resides. The default name of the volume is *(#VOLUME)*.
6. Submit the IWNCRHFS job.

Configuring the IWNIMNT job
You can mount the z/OS File System (zFS) that is created by the IWNCRZFS job, by configuring and submitting the IWNIMNT job. You can choose to create and mount a hierarchical file system (HFS) instead, by using the IWNCRHFS job and updating the IWNIMNT job as needed.

The IWNIMNT job creates, and then mounts the zFS or HFS at the mount point.

1. Locate the IWNIMNT job in the SYS1.SAMPLIB data set and open it.
2. Modify the following values on your system, being sure to update the *-PathPrefix-* to match your system configuration.

   Note: You can use either a HFS or ZFS. However, the following sample job pertains only to those customers who are using a zFS.

```
//**********************************
//*
//IWNIMNT  EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
   PROFILE WTPMSG MSGID
   TIME

   /* Make sure mountpoints exist. */
    MKDIR '-PathPrefix-/opt/IBM'               MODE(7,5,5)
    MKDIR '-PathPrefix-/opt/IBM/CSM'            MODE(7,5,5)

   /* Mount the zFS or HFS. */
    MOUNT FILESYSTEM('#CSM.ZFS') TYPE(ZFS) +
          MODE(RDWR) +
          MOUNTPOINT('-PathPrefix-/opt/IBM/CSM')
   /*
```

3. Specify the zFS or HFS that is created by either the IWNCRZFS or IWNCRHFS job by editing the **MOUNT FILESYSTEM** (*#CSM.ZFS*) parameter and the **TYPE** parameter.
4. Specify *CSM_ProductionRoot* as the mount point by editing the **MOUNTPOINT** parameter. The default mount point is *-PathPrefix-*/opt/IBM/CSM.
5. Submit the IWNIMNT job.

Configuring the IWNINSTL job
To set up the data source, applications, security, Java virtual machine, and the libraries in WebSphere Application Server for z/OS Liberty Profile, configure, and submit the IWNINSTL installation job.

The ID that runs the IWNINSTL job must have an OMVS segment in RACF with a memory limit (*MEMLIMIT*) of 4G or more. Also, the *MEMLIMIT* set in the IWNINSTL job must have a MEMLIMIT of 4G or more and a REGION size set to 0 (to allow as much memory as it needs).

The IWNINSTL job must be run for the initial Copy Services Manager installation, and for any Copy Services Manager upgrade on z/OS.

To configure the IWNINSTL job with the correct installation information, follow these steps:

1. Locate the IWNINSTL job in the SYS1.SAMPLIB data set and open it.
2. Find the strings as shown in the following example, and edit the values for your environment:

```
CLASSPATH=-PathPrefix-/usr/lpp/IBM/CSM/scripts
CSM_USER=#csm_user
CSM_GRP=#csm_grp
CSM_InstallRoot=-PathPrefix-/usr/lpp/IBM/CSM
CSM_ProductionRoot=-PathPrefix-/opt/IBM/CSM
TIME_ZONE=GMT
CLIENT_PORT=9560
HA_PORT=9561
GUI_PORT=9559
AUTH_PORT=9562
ENABLE_LDAP=false
//*CSM_ADDR_OWNER=#csm_addr_owner
/*
```

CLASSPATH
> An environment variable that defines the location of the Copy Services Manager installation binary files and scripts.

CSM_USER
> The user ID for Copy Services Manager. This user ID is used to log on to the Copy Services Manager GUI and CLI.
>
> **Note:** It is suggested that you make this user ID the same as the one that is defined in the IWNRACF1 job. For more information, see "Configuring the IWNRACF jobs" on page 5.

CSM_GRP
> The ID for the group that the user belongs to.

CSM_InstallRoot
> The location in which Copy Services Manager was installed by the SMP/E APPLY step. The data in this location is read only.
>
> Do not change the *CSM_InstallRoot* or *CSM_ProductionRoot* paths in the job other than to modify the `path_prefix` directory. If you modify the `path_prefix` directory, verify that the directory exists in UNIX System Services (USS).

CSM_ProductionRoot
> The location in which Copy Services Manager stores the database and command line. Data that requires read and write access must be in this path.

TIME_ZONE
> The time zone that is used by Java virtual machine. The default is GMT, which is Greenwich mean time.
>
> If you do not include a value for the **TIME_ZONE** parameter, the default is GMT.

CLIENT_PORT
> The client port that is used by the CLI to communicate with the Copy Services Manager server. The default value is 9560.

HA_PORT
> The standby management server port that is used for communication between the active and standby management server in a high-availability relationship. The default value is 9561.
>
> **Restriction:** In a high-availability relationship, the client and standby management server port numbers must be the same on both the management server and the standby management server. If you change the client port number on either the management server or the standby management server, you must also change the port number on the other server.

GUI_PORT
> The port that is used to access the Copy Services Manager server with the url: `https://<host_name>:<GUI_PORT>/CSM/`. The default value is 9559.

AUTH_PORT
> The port that is used for authentication to the Copy Services Manager server. The default value is 9562.

***ENABLE_LDAP*= TRUE | FALSE**

If you plan on using LDAP on your system for authentication, you need to enable LDAP by updating the parameter ENABLE_LDAP=TRUE. You also need to define a started task in IWNRACF2, and copy the IWNAUTH sample procedure to SYS1.PROCLIB. See "Configuring the IWNRACF jobs" on page 5, and "Configuring the IWNAUTH job" on page 22 for more information.

CSM_ADDR_OWNER

Globally change CSM_ADDR_OWNER to the user ID that is associated with the Copy Services Manager address space. It should be the same ID that was defined in IWNRACF2 if you ran that job. See "Configuring the IWNRACF jobs" on page 5 for more information.

For an in-place upgrade from Tivoli Storage Productivity Center for Replication to Copy Services Manager, the following two additional parameters can be added:

```
TPCR_ProductionRoot=path_prefix/opt/Tivoli/RM
KEEP_TPCR=false
```

TPCR_ProductionRoot

Specifies the production root that was used when Tivoli® Storage Productivity Center for Replication was installed. Update this path to indicate what directory path for Copy Services Manager to use for the upgrade.

***KEEP_TPCR*= TRUE | FALSE**

Default is KEEP_TPCR=false. If set to true, when you upgrade from Tivoli Storage Productivity Center for Replication to Copy Services Manager, the TPCR directory structure is not deleted.

3. Optional: Add the following JCL to the job so that the installation log and error files are written to the job output.

```
//*************************************
//* PRINT OUT LOG AND ERROR INFO
//*************************************
//LOGOUT EXEC PGM=IKJEFT01,DYNAMNBR=300,COND=EVEN
//SYSTSPRT DD SYSOUT=*
//HFSOUT DD PATH='PATH='path_prefix/etc/install_CSM.log'
//HFSERR DD PATH='PATH='path_prefix/etc/install_CSM_err.log''
//STDOUTL DD SYSOUT=*,DCB=(RECFM=VB,LRECL=133,BLKSIZE=137)
//STDERRL DD SYSOUT=*,DCB=(RECFM=VB,LRECL=133,BLKSIZE=137)
//SYSPRINT DD SYSOUT=*
//SYSTSIN DD *
OCOPY INDD(HFSOUT) OUTDD(STDOUTL)
OCOPY INDD(HFSERR) OUTDD(STDERRL)
/*
```

4. Submit the IWNINSTL installation job.

After the IWNINSTL job is complete, look for any return codes. The return codes 0 and 1 are acceptable. For other job return codes, see the following error and log files:

```
//HFSOUT DD PATH='PATH='path_prefix/etc/install_CSM.log'
//HFSERR DD PATH='PATH='path_prefix/etc/install_CSM_err.log''
```

You can also locate the *path_prefix*/etc/ directory by using iShell or use the OMVS command line. Then, look for the log files to identify any errors that might occur.

TROUBLESHOOTING: In the event of a failed initial installation, perform the following steps to add the FORCE_FULL_INSTALL parameter in the IWNINSTL job:

⚠️ **Attention:**

This option is to be used only if there has been a failed initial installation and not for upgrades.

When IWNINSTL is submitted with this parameter, the option replaces all the contents of the properties folder and overwrites any user customizations that have been made.

1. Make a backup of the Copy Services Manager database using the procedure described in the *Copy Services Manager User's Guide,* Chapter 2. Administering in the section titled "Backing up and restoring

product data." See <u>"Publications and related information" on page viii</u> for details on how to locate this guide.

2. Stop IWNSRV started task (if not already stopped). See <u>"Configuring the IWNSRV job" on page 21</u> for more information.

3. If you are using LDAP to manage users, stop the IWNAUTH started task. See <u>"Configuring the IWNAUTH job" on page 22</u> for more information.

4. Edit the IWNINSTL job: Force a replacement of base properties files and settings by appending the following flag to the sample job "IWNINSTL" **FORCE_FULL_INSTALL=TRUE|FALSE**

   Notes:

   - This option can be appended anywhere between the //STDENV DD * and /* ending statement of the JCL so that it is passed in as an environment variable to BPXBATCH.

   - When set to TRUE, this option takes effect. If set to FALSE, the option has the same effect as not having the option in the IWNINSTL JCL.

5. Back up your existing properties files located at:

   ```
   <Path Prefix>/opt/IBM/CSM/wlp/usr/servers/csmServer/properties
   ```

6. Submit the IWNINSTL job to update the application and reset the properties values. The existing copy services, attached devices, and session configuration will be saved.

7. Start IWNSRV started task.

8. If you are using LDAP to manage users, start IWNAUTH started task.

Configuring the IWNSRV job

Edit the IWNSRV job and copy it to the PROCLIB system library with the correct directory paths to start and stop IBM Copy Services Manager.

After you run the IWNRACF and IWNINSTL jobs, you configure the IWNSRV job. To start Copy Services Manager through the console, issue the **Start IWNSRV** command. To stop Copy Services Manager, issue the **Stop IWNSRV** command.

1. Edit the *path_prefix* variable in the following directory path, with the correct information for your environment:

   ```
   //*------------------------------------------------------------------
   //  SET INSTDIR='path_prefix/opt/IBM/CSM/wlp'
   //  SET USERDIR='path_prefix/opt/IBM/CSM/wlp/usr'
   //*------------------------------------------------------------------
   ```

   where:

   INSTDIR

   The directory path to the WebSphere Application Server for z/OS Liberty Profile server installation. This path is used to find the product code.

   USERDIR

   The directory path to the WebSphere Application Server for z/OS Liberty Profile server user area. This path is used to store shared-and server-specific configuration information.

2. If you want the job to output log information to z/OS UNIX System Services, uncomment and edit the *STDENV* variable.

   ```
   //* Start the server
   //*------------------------------------------------------------
   //STEP1    EXEC PGM=BPXBATSL,REGION=0M,TIME=NOLIMIT,
   //  PARM='PGM &INSTDIR./lib/native/zos/s390x/bbgzsrv &PARMS'
   //WLPUDIR  DD PATH='&USERDIR.'
   //STDOUT   DD SYSOUT=*
   //STDERR   DD SYSOUT=*
   //*STDENV   DD PATH='/etc/system.env',PATHOPTS=(ORDONLY)
   //*STDOUT   DD PATH='&ROOT/std.out',
   //*         PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
   //*         PATHMODE=SIRWXU
   //*STDERR   DD PATH='&ROOT/std.err',
   ```

```
//*          PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//*          PATHMODE=SIRWXU
//*
```

where:

WLPUDIR

The DD PATH that points to the WebSphere Application Server for z/OS Liberty Profile server USERDIR directory. If the DD PATH is not allocated, the USERDIR directory location defaults to the `wlp/usr` directory in the installation tree view.

STDOUT

The destination for the STDOUT variable (DD SYSOUT - System.out).

STDERR

The destination for the STDERR variable (DD SYSOUT - System.err).

STDENV

In the initial UNIX environment, this path is read by the system. The installation default and specific server environment files are merged into this environment before the Java Virtual Machine is started.

Configuring the IWNAUTH job

Edit the IWNAUTH job and copy it to the PROCLIB system library with the correct directory paths to start and stop Copy Services Manager authentication.

After you run the IWNRACF and IWNINSTL jobs, and you start IWNSRV, you configure the IWNAUTH job. To start Copy Services Manager authentication through the console, issue the **Start IWNAUTH** command. To stop Copy Services Manager authentication, issue the **Stop IWNAUTH** command.

Note: For z/OS, the IWNAUTH service is optional to run.

1. Edit the *path_prefix* variable in the following directory path, with the correct information for your environment:

```
//*-----------------------------------------------------------------
// SET INSTDIR='path_prefix/opt/IBM/CSM/wlp'
// SET USERDIR='path_prefix/opt/IBM/CSM/wlp/usr'
//*-----------------------------------------------------------------
```

where:

INSTDIR

The directory path to the WebSphere Application Server for z/OS Liberty Profile server installation. This path is used to find the product code.

USERDIR

The directory path to the WebSphere Application Server for z/OS Liberty Profile server user area. This path is used to store shared-and server-specific configuration information.

2. If you want the job to output log information to z/OS UNIX System Services, uncomment and edit the *STDENV* variable.

```
//* Start the server
//*------------------------------------------------------------
//STEP1    EXEC PGM=BPXBATSL,REGION=0M,TIME=NOLIMIT,
//   PARM='PGM &INSTDIR./lib/native/zos/s390x/bbgzsrv &PARMS'
//WLPUDIR  DD PATH='&USERDIR.'
//STDOUT   DD SYSOUT=*
//STDERR   DD SYSOUT=*
//*STDENV   DD PATH='/etc/system.env',PATHOPTS=(ORDONLY)
//*STDOUT   DD PATH='&ROOT/std.out',
//*          PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//*          PATHMODE=SIRWXU
//*STDERR   DD PATH='&ROOT/std.err',
//*          PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//*          PATHMODE=SIRWXU
//*
```

where:

WLPUDIR
> The DD PATH that points to the WebSphere Application Server for z/OS Liberty Profile server USERDIR directory. If the DD PATH is not allocated, the USERDIR directory location defaults to the `wlp/usr` directory in the installation tree view.

STDOUT
> The destination for the STDOUT variable (DD SYSOUT - System.out).

STDERR
> The destination for the STDERR variable (DD SYSOUT - System.err).

STDENV
> In the initial UNIX environment, this path is read by the system. The installation default and specific server environment files are merged into this environment before the Java Virtual Machine is started.

Installing on distributed systems

Install Copy Services Manager by running the installation package that is provided with your license.

1. Close all open applications before installation.
2. Run the installation setup file that is provided with your license.

   - AIX: `csm-setup-6.2.x-aix.bin`
   - Linux: `csm-setup-6.2.x-linux-x86_64.bin`
   - Linux on z Systems: `csm-setup-6.2.x-linux-s390x.bin`
   - PowerPC Linux: `csm-setup-6.2.x-linux-ppc.bin`
   - Windows: `csm-setup-6.2.x-win.exe`

   Note: If you installed an earlier version of Copy Services Manager, the installation setup file automatically upgrades to the most-recent version.

3. Select the appropriate language from the bottom menu of the IBM Copy Services Manager installation page, and click **OK**.
4. An **Introduction** page is displayed. Review the text, and click **Next** to proceed.
5. The **Select License** page displays. It gives you the option to provide your license here instead of after the installation. Click **Browse** to select a license `zip` file to apply, and click **Next**.

   Note: If no license file is available, click **Skip** to apply an evaluation license. You can apply a full license later.

6. Review the license text and select **I accept the terms in the license agreement** to proceed to the next step in the installation. You can also **Print** the license agreement. When you are finished making selections, click **Next** to go to the next page.

   Note: If you select **I do not accept the terms in the license agreement**, a dialog prompts you to confirm this selection. If you do confirm it and click **Yes**, the installation process ends and Copy Services Manager is not installed.

7. On the **Select Installation Type** page, select one of the following options, and click **Next**:

   - Install
   - Migrate or restore by using existing backup

     See Chapter 4, "Migrating Copy Services Manager," on page 41 for migration details.

8. Provide the information that is requested on the installation setup pages. Click **Next** when you are ready to proceed.

   a) Choose an installation folder, or accept the default.

      Note: You can also click to **Restore Default Folder**.

b) For authentication information, define a user name or accept the default, `csmadmin`, and define and confirm a password.

c) For server port configuration, use the default ports, or define different ports that are not in use. See Table 5 on page 2 for port information.

Note: You can also click to **Restore Defaults**.

9. Confirm the information on the **Pre-Installation Summary** page. Return to **Previous** pages to modify the information if needed, and click **Install**.

10. After the installation completes, a message is displayed that the installation is successful. Click **Done**.

11. If a browser is installed, you are asked whether you want to start the browser to access the Copy Services Manager GUI. Otherwise, access the GUI by opening a browser and pointing to `https://host_name:9559/CSM/`.

Note: After you log in to the GUI, you are presented with a warning page, **This Connection is Untrusted**, regarding an invalid security certificate.

a. Click **Add Exception**.

b. On the **Add Security Exception** page, click **Confirm Security Exception**.

c. Log in to the GUI with the user name and password that you defined during the installation.

If you install Copy Services Manager on a distributed system, and are managing HyperSwap, you also need to run the following IWNRACF jobs:

- IWNRACF3: HyperSwap address spaces
- IWNRACF4: HyperSwap Sockets Server address space
- IWNRACF5: Copy Services Manager host connection ID

For more information, see "Configuring the IWNRACF jobs" on page 5.

Silent installation

You can complete a silent installation of Copy Services Manager by using the response file, `silent_CSMInstall.properties`, provided with the installation image. A silent installation is useful when remotely accessing a Linux or AIX system without a graphical user interface.

You can change the values in the response file. The only required parameter and associated value is:

```
LICENSE_ACCEPTED=true
```

Note: If you have the license file, you also need to set the CSM_LICENSE_FILE parameter to the path where the license file is located:

```
CSM_LICENSE_FILE=<path to license .zip file>
```

(In the response file, LICENSE_ACCEPTED is set to false.) This value installs Copy Services Manager with the following default values:

- Ports:
  - 9559
  - 9560
  - 9561
  - 9662
- Installation directory path:
  - Windows: `C:/Program Files/IBM/CSM`
  - Linux/AIX: `/opt/IBM/CSM`
- User name: *csmadmin*

- Password: *passw0rd*

The following example silent installation is for Windows.

1. Open a command prompt.
2. Change directories to where the `setup.exe` file is located. Or, you can point to the relevant directory.
3. Enter the following command:

   cmd /c *copy_services_manager_setup.exe* **-i silent -f** *silent_installation_response_file*

   For example: **cmd /c csm-setup-6.1.x-win.exe -i silent -f silent_CSMInstall.properties**

   Notes:

   a. When you issue a silent installation in a Windows command prompt, the command line returns immediately. To pause a return to the command line until the installation completes, prefix the silent installation command string with **cmd /c**.
   b. Failure messages are printed to the screen on Linux systems but not on Windows. However, for Windows, you can modify the value for `LOG_LOCATION=`*a_directory* in the response file to record failure information for Windows.
   c. On Linux systems, you can direct messages to a `.txt` file. For example, append **>** *name_of_install_log.txt* to the command string in step <u>"3" on page 25</u>.

Exporting a license file

You can export a license (`.zip`) file from the Copy Services Manager GUI that contains the installed product licenses.

You can use the export license feature to transfer full licensed support to another server.

Use these steps to export a license (`.zip`) file from the Copy Services Manager GUI:

1. Log in to the Copy Services Manager GUI as a user with administrative privileges.
2. In the menu bar, click **Settings** > **Advanced Tools**. The **Advanced Tools** panel is displayed.
3. Scroll down to locate the `Copy License Key or Export License` section of the panel. Click **Export**.

   Note: If no license file is available for export, a status message is displayed saying so.

   When you click **Export**, the server creates and stores a compressed (`.zip`) file of all the license information in the *<path_prefix>*`/csmServer/license` directory.

   When the license data is exported, the file name and location on the management server appears as a link. You can click the link to download the exported licenses to the server on which the web browser is running. You can import the file when you click **Update Licenses** from the Copy Services Manager GUI on another server. For information on how to import a license, see <u>"Applying license files after installation or migration, or updating licenses" on page 26</u>.

Copying a license key

The Copy Services Manager GUI supports the ability to import a string-based key for transferring a license to another server.

You can use the copy license key feature to transfer full licensed support to another server.

Use these steps to copy a license key from the Copy Services Manager GUI:

1. Log in to the Copy Services Manager GUI as a user with administrative privileges.
2. In the menu bar, click **Settings** > **Advanced Tools**. The **Advanced Tools** panel is displayed.

3. Scroll down to locate the `Copy License Key or Export License` section of the panel. Click the displayed string value, or the **Copy License Key** button, to copy the license key string to the clipboard to enable another server.

   You can import the license key when you click **Update Licenses** from the Copy Services Manager GUI on another server. For information on how to import a license, see "Applying license files after installation or migration, or updating licenses" on page 26.

Applying license files after installation or migration, or updating licenses

After you install or migrate to Copy Services Manager, you must apply the available license files if you did not do so during the installation process. This task can also be used to update licenses, such as for transfer to another server.

Contact your IBM representative to either obtain a Try-and-Buy key, or to determine where the license files are stored for your version of Copy Services Manager. The license enablement files, which contain the license keys to be applied, are stored within the ordering system that you used. You need to download the files from this location.

If you want to import a license to transfer licensed support to another server, you must first export the license (`.zip`) file. See "Exporting a license file" on page 25 for more information before you follow the procedure to apply the license file. Alternatively, you can import a license key string if your system does not support importing a license file, for example when Copy Services Manager is installed on the DS8000 HMC. The license key works like the Try-and-Buy activation key. See "Copying a license key" on page 25 for more information.

The following steps detail how to apply Copy Services Manager license files after installation or migration, or how to update licenses, such as for transfer to another server.

Use these steps to apply or update license files:

1. If necessary, download the appropriate license files as instructed by your IBM representative. These files are in compressed (`.zip`) file format.
2. Log in to the Copy Services Manager GUI as a user with administrative privileges.
3. In the menu bar, on the far right, click **Update Licenses**.

   Note: This menu option only appears when there is no Try-and-Buy key and no full license applied. If either of those items are applied, this menu option disappears.

   - You can also click **Settings** > **Administration** to get to the **Update Licenses** button. This button appears on the **Administration** page if either no license files are applied, or only the Try-and-Buy license is applied. The button disappears only after you upload the full license compressed (`.zip`) file.

4. Update the license by either typing in the activation key or uploading a license file. The activation key is a string value that is provided for Try-and-Buy capabilities by your account representative, or through an export licenses action on an existing installation. If a license file was provided for activation, such as a `csm-license.zip` file, click the **Click here to activate the product by using the key file** text, and then click **Browse** to select a license file to upload.
5. Click **Apply** to submit, or click **Cancel** to exit without applying any licenses.

When the necessary license files are applied, the available functions are enabled for use.

Switching out the default Copy Services Manager certificates

You can switch out the default certificates that are supplied by Copy Services Manager.

To switch out the default certificates, you need to change two main files: `etc/csmKeyStore.jks` and `etc/csmTrust.jks`. These files are at:

- *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/etc/ for z/OS

- *install dir*/liberty/wlp/usr/servers/csmServer/etc/ for distributed

You can create new versions of these files by using iKeyman, which is distributed with the Copy Services Manager version of Java.

Notes:

- You can locate the iKeyman tool at *install dir*/liberty/wlp/IBM/Java/jre/bin/ikeyman (or ikeyman.exe on Windows).
- The iKeyman tool is not available on z/OS. Therefore, you must first complete this procedure on a distributed system, and then upload the changes to the z/OS server. The JKS files need to be uploaded to z/OS UNIX System Services in a binary format.

Restriction: You cannot follow this procedure to switch out the default certificates when Copy Services Manager is installed on the DS8000 HMC.

Follow these steps to switch out the default certificates that are assigned by Copy Services Manager:

1. Back up the original versions of the csmKeyStore.jks and csmTrust.jks files to a new directory. These files are currently at:

    - *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/etc/ for z/OS
    - *install dir*/liberty/wlp/usr/servers/csmServer/etc/ for distributed systems

2. In iKeyman, select **Key Database File** > **New** to create a new csmKeyStore.jks file, and provide a password for it.

    Note: Save the new file to a different location from the existing version of the file so that you do not overwrite it.

3. In iKeyman, select **Key database content** > **Personal Certificates** > **New Self-Signed** to generate a new self-signed certificate. Or, you can choose to import a private key, by selecting **Import**.

    a) Use a key size of at least 2048 for a new self-signed certificate.

    b) The iKeyman tool suggests an SHA-1 signing algorithm, and a one-year expiration by default. Change this algorithm to a more-secure signature algorithm. A signature algorithm of SHA256WithRSA, and an extended expiration date are recommended.

    c) Assign a label to the self-signed certificate. For example, you might want to use one like csmservercustom to show that you are using something different from the default.

4. Then, click **Extract Certificate**. Either option works for the **Data type** entry. Export the certificate as csmserverdfault.arm, which is the public certificate information.

5. Create a new JKS file to replace csmTrust.jks by selecting **Key Database File** > **New**, and provide a password for it.

    Note: Save the new file to a different location from the existing version of the file so that you do not overwrite it.

6. In the **Key database content** menu, change the selection to **Signer Certificates**. Click **Add** to add the extracted certificate, csmserverdfault.arm, and give it the same label as you did in step "3.c" on page 27, such as csmservercustom.

    The iKeyman tool automatically saves your information.

7. Move the new csmKeyStore.jks and csmTrust.jks files that you re-created with the iKeyman tool, into the original directories.

8. Back up a copy of your rmserver.properties file, which is at:

    - *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/properties for z/OS
    - *install dir*/liberty/wlp/usr/servers/csmServer/properties for distributed systems

    Locate the default sections of the file as shown in the code sample that follows. Uncomment and update the password for the following options as shown:

```
#  *Used to setup SSL sockets between the clients and server.
#communications.keyStore=etc/csmKeyStore.jks
```

```
communications.keyStorePwd=<Password for csmKeyStore.jks>

#  *Used so that Clients can authenticate with the server using Certificates.
#communications.authStore=etc/csmTrust.jks
communications.authStorePwd=<Password for csmTrust.jks>
```

9. Back up a copy of your `csmConnection.properties` file, which is at:

   - *path_prefix*`/opt/IBM/CSM/wlp/usr/servers/csmServer/properties` for z/OS
   - *install dir*`/liberty/wlp/usr/servers/csmServer/properties` for distributed systems

   Update this file to make **csm.server.certificate** the alias of the `csmTrust.jks` file. Use the label that you assigned to the self-signed certificate, as you created in step "3.c" on page 27, such as `csmservercustom`.

   ```
   csm.server.certificate=csmservercustom
   ```

10. Restart Copy Services Manager for the changes to take effect.
11. The next steps involve the CLI. Copy the `csmTrust.jks` file to the Copy Services Manager CLI directory at *install dir*`/CLI/`.
12. Next, create a properties directory in the CLI directory (`CLI/properties`).
13. Create a `csmclient.properties` file in the properties directory (so the path is `CLI/properties/csmclient.properties`) with the following content:

    ```
    communications.trustStore=csmTrust.jks
    communications.trustStore.password=<assigned password>
    ```

    Note: The default `csmTrust.jks` file is embedded in the `csmcli.jar`. You cannot remove it. Use the `csmclient.properties` file to point it to a different location.

14. Then, log in to the Copy Services Manager CLI.
15. Optional: Repeat the CLI steps if you have the stand-alone CLI extracted on other systems in your environment.
16. Edit the `bootstrap.properties` file to point the server to use the new `csmTrust.jks` file that contains the SSL certificate, as shown:

    ```
    keystore_location=csmTrust.jks
    keystore_password=<assigned password>
    ```

    Otherwise, it defaults to use a `key.jks` file in the `/resources/security` directory.

    See the "bootstrap.properties file" on page 49 for more information.

The default certificates that are supplied by Copy Services Manager are switched out.

Installing the command-line interface on a remote system

You can install the Copy Services Manager CLI to run on a remote system.

To install the Copy Services Manager CLI on a remote system, you must download and extract the appropriate compressed files for your software level and operating system to the proper location.

1. Download the Copy Services Manager CLI installation package (`csm-CLI`) for your version and system type to the remote server where you want to run the command line.

   This file package can be obtained from the same location as the other Copy Services Manager installation files. The available package types and associated file names are listed in the following table:

Table 6. Copy Services Manager CLI installation package file names by operating system

Operating system	Copy Services Manager CLI installation package file name
Windows	`csm-CLI-6.2.x-win.zip`
AIX	`csm-CLI-6.2.x-aix.tar.gz`
Linux 64-bit PowerPC® and Power Architecture®	`csm-CLI-6.2.x-linux-ppc.tar.gz`
Linux on z Systems	`csm-CLI-6.2.x-linux-s390x.tar.gz`
RedHat or SuSE Linux	`csm-CLI-6.2.x-linux-x86_64.tar.gz`
z/OS	`csm-CLI-6.2.x-zos.pax`

2. Extract the `csm-CLI` file package to a directory on the remote system, referred to in the following steps as the *CSM_CLI_DIR* directory: For Windows, extract the files by right-clicking and selecting **Extract All**. For AIX or Linux, use the **gunzip**, and then **tar** commands to extract the files. For z/OS, extract the files by using the **pax** command.

3. **For z/OS only:** After extracting files using the **pax** command, there is an additional step to set file attributes on Java libraries that the CLI uses:

```
extattr +a CSM_CLI_DIR/csm/Java/lib/s390x/compressedrefs/libj9ifa29.so
```

```
extattr +a CSM_CLI_DIR/csm/Java/lib/s390x/default/libj9ifa29.so
```

4. Open the *CSM_CLI_DIR*/csm/CLI directory.

5. Edit the `repcli.properties` file by typing the server name and port of your Copy Services Manager server. The default setting in the file is shown:

```
server=localhost
port=9560
```

The updated setting in the file appears as follows:

```
server=myCSMserver.domain.com
port=9560
```

Where *myCSMserver.domain.com* correlates to the Copy Services Manager server name in your environment.

Note: Port 9560 is the default port that is used during Copy Services Manager installation. If you used a custom port, you must change the port setting.

6. Start the Copy Services Manager CLI by entering the **csmcli.bat** command for Windows, or the **csmcli.sh** command on AIX, Linux, or z/OS systems. Enter the associated Copy Services Manager user name and password. See the following example:

```
C:\temp\csm-CLI-6.2-win\csm\CLI>csmcli.bat
Please enter a username for logging onto the server
csmadmin
Please enter a password for logging onto the server
>
IBM Copy Services Manager Command Line Interface (CLI)
 Copyright 2007, 2012 IBM Corporation
 Version: 6.2
 Build: a20150818-0519
 Server: csmwin2k12     Port: 9560    UseREST: false
 Authentication file: csmcli-auth.properties

csmcli>
```

The Copy Services Manager CLI is now configured to run on the remote system.

Configuring additional features

After you complete the postinstallation tasks, you can configure additional features to add more functions to your Copy Services Manager environment.

The following topics provide instructions for Copy Services Manager to connect to a z/OS host system. The Copy Services Manager server can be running on either a different z/OS server or a Copy Services Manager server.

Enabling a host name or IP address connection to a z/OS host system

You can use a host name or IP address to connect to IBM z/OS host systems in Copy Services Manager regardless of the operating system on which the application is installed.

You can connect to a z/OS host system from Copy Services Manager that is running on Windows, Linux, AIX, or z/OS. When you are connected to a host system, you can manage HyperSwap sessions that are running on the system. In addition, a single instance of Copy Services Manager is used to manage multiple HyperSwap instances that are running in different z/OS systems and sysplexes.

The following steps set the required Resource Access Control Facility (RACF®) settings on the host system, and define the **SOCKPORT** parameter when the HSIB HyperSwap management address space is started, using PGM=IOSHMCTL.

To connect to a z/OS host system from Copy Services Manager, use these steps:

1. Follow the procedure for the IWNRACF3, IWNRACF4 and IWNRACF5 jobs in "Configuring the IWNRACF jobs" on page 5.
2. After you configure RACF for an IP connection, you can start the HSIB address space with the **SOCKPORT** parameter as shown in the following example:

```
//HSIB     JOB MSGLEVEL=(1,1),TIME=NOLIMIT,REGION=0M
//IEFPROC EXEC PGM=IOSHMCTL,PARM='SOCKPORT=port_number'
```

where $port\_number$ is a number in the 1 - 65535 range. You must enter this port number when you add the z/OS host system to Copy Services Manager.

For more information about RACF commands, see the *z/OS V2R2.0 Security Server RACF Command Language Reference* at https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.2.0/com.ibm.zos.v2r2.icha400/toc.htm.

Preparing to use HyperSwap from z/OS

Before you can use HyperSwap with Copy Services Manager, you must configure z/OS to use HyperSwap.

Configuring HyperSwap

On IBM Z, HyperSwap requires that all RESERVEs are converted to global enqueues (ENQs).

When a HyperSwap is initiated and a RESERVE exists on any PPRC device, the RESERVE might be lost.

To prevent data integrity exposure, configure global resource serialization (GRS) to convert RESERVEs to Global ENQs, use these steps:

1. Run the ENQ/RESERVE/DEQ Monitor with filtering REQTYPE of NCRESERVE to gather reports on non-converted RESERVEs issued by the system. For more information about using the ENQ/RESERVE/DEQ monitor tool, see the *z/OS MVS™ Planning: Global Resource Serialization* document.
2. Use the GRSRNLxx member of SYS1.PARMLIB statement to add an RNLDEF customization parameter.
3. To convert any RESERVE that might be issued against volumes that are managed by HyperSwap to Global ENQs, use a PATTERN entry.
4. Use the RNLDEF parameter to convert all RESERVEs to Global ENQs: RNLDEF RNL(CON) TYPE(PATTERN) QNAME(*).

For more information about converting RESERVEs to Global ENQs, see the section about GRSRNLxx (global resource serialization resource name lists) in the most-recent version of the *z/OS MVS Initialization and Tuning Reference*.

When RESERVEs are converted to GRS Global ENQs, the ENQs might take longer to resolve if the ISGLOCK structure is too small to process each global ENQ independently. If this situation occurs, you might want to increase the size of your ISGLOCK structure. For information about GRS, including guidelines on how to resize your ISGLOCK structure, see the latest version of the *z/OS MVS Planning: Global Resource Serialization* document.

Sharing the HyperSwap managed devices outside of the sysplex

When HyperSwap is started, the cross-system coupling facility or XCF is used to coordinate all the systems in the sysplex through the swap. Any system outside the sysplex does not participate in the swap, and is unaware that the device was swapped. In certain cases, the system outside the sysplex continues to use the old primary volumes after a swap, that results in data integrity exposures.

The HyperSwap address spaces

HyperSwap requires two address spaces: the HyperSwap API address space, and the HyperSwap management address space. Follow these steps to start the address spaces:

1. Add procedures for the address spaces to the SYS1.PROCLIB data set:

   For the HyperSwap API address space:

   ```
   //HSIBAPI JOB MSGLEVEL=(1,1),TIME=NOLIMIT,REGION=0M
   // EXEC PGM=IOSHSAPI
   ```

   For the HyperSwap management address space:

   ```
   //HSIB JOB MSGLEVEL=(1,1),TIME=NOLIMIT,REGION=0M
   // EXEC PGM=IOSHMCTL
   ```

   Note: If you are enabling an IP connection, the **SOCKPORT** parameter also needs to be added for the HyperSwap management address space, as shown in the following example.

   ```
   //HSIB JOB MSGLEVEL=(1,1),TIME=NOLIMIT,REGION=0M
   // EXEC PGM=IOSHMCTL,PARM='SOCKPORT=5858'
   ```

2. Start the address spaces in one of the following ways:

   - Issue the **START** command manually.
   - Include the **START** command in the COMMND*xx* member of the SYS1.PARMLIB data set.

   Note: When you issue the START commands, either manually or by using COMMNDxx, it is preferred, although not required, that you start the API address space before the management address space.

These are the START commands for the specific address spaces:

For the HyperSwap API address space start command:
   ```
   START HSIBAPI,SUB=MSTR
   ```
For the HyperSwap management address space start command:
   ```
   START HSIB,SUB=MSTR
   ```

To reduce the possibility of a swap failure because of page faults, enable the CRITICALPAGING function. To enable the CRITICALPAGING function, use the FUNCTIONS statement of the COUPLE*xx* PARMLIB member for each system in the sysplex.

For example, add the following CRITICALPAGING statement to the COUPLE*xx* PARMLIB member:

```
FUNCTIONS ENABLE(CRITICALPAGING)
```

Tip: You cannot enable the CRITICALPAGING function through the **SETXCF** command. However, you can use either method to stop CRITICALPAGING.

For information about indicating the address spaces that are critical for paging, see the *z/OS V1R12.0 MVS Initialization and Tuning Reference* document.

SMF Recording

When z/OS HyperSwap is active, there is no SMF interval recording for the HyperSwap address spaces. There is no SMF interval recording for either the HSIB or HSIBAPI address spaces, or for the XCFAS address spaces. The reason for this design is to avoid potential hangs during HyperSwap processing due to access to disk storage by SMF. If you have existing SMF processes that depend on SMF interval records for XCFAS, review and revise these procedures.

Gathering information or controlling a HyperSwap session by using commands

When you are running HyperSwap, you can use extra commands to gather information or control a HyperSwap session on z/OS.

Table 7. Extra HyperSwap commands on z/OS

Command	Result
D HS,STATUS	Displays the status of a HyperSwap session. This command also displays any reasons why HyperSwap might be disabled, and the policies for the HyperSwap session.
D HS,CONFIG(DETAIL,ALL)	Displays the detailed configuration for the HyperSwap session. The volumes and status of all pairs in the HyperSwap configuration are listed.
SETHS SWAP	Starts a planned HyperSwap session. You can issue this command instead of issuing the **HyperSwap** command from Copy Services Manager.
SETHS DISABLE	Disable HyperSwap by operator command. This command prevents a HyperSwap session from occurring, either by command or automatically.
SETHS ENABLE	Enable HyperSwap by operator command. This command allows a HyperSwap session to be performed, either by command or automatically, if a HyperSwap session is not disabled for other reasons.
SETHS RESUMEIO	Resumes normal I/O activity to devices after a suspended HyperSwap action because the Hold I/O option was used.

Configuring a secure communication between HyperSwap and the client

Create a certificate authority (CA) for TLS and prepare the CA for export to the client for server certificate authenticity.

The Copy Services Manager server communicates through the TCP/IP protocol. This protocol is encrypted by Transport Layer Security (TLS) to a HyperSwap management-address space that you can use to manage your attached storage devices. You can manage the HyperSwap and z/OS hardened freeze functions on these devices.

Important: When you create the CA, the user ID that you use for your commands must be the same user ID that is used to run HyperSwap.

1. To create a CA and prepare it for export, find the sample job in `wlp/usr/servers/csmServer/etc/CERTCRE8.sample` and modify the parameters as necessary for your environment.
2. Copy this job to SYS1.CLIST(CERTCRE8) and run it.
3. Download the file that you exported in CERTCRE8, in binary, to your local file system. Then, it is available for import on the Copy Services Manager GUI for "Importing a certificate for a z/OS host connection by using the GUI" on page 33.

Importing a certificate for a z/OS host connection by using the GUI

You can upload a certificate for a z/OS host connection from within the Copy Services Manager GUI.

You can use the certificate file that was exported in "Configuring a secure communication between HyperSwap and the client" on page 32 to import for this task.

Log in to the Copy Services Manager GUI and go to **Storage** > **Host Connections**. You can add the certificate to a new host connection, or update an existing, disconnected host connection.

Adding a new z/OS host connection

You can import a certificate to add a new z/OS host connection.

To import a certificate for a new z/OS host connection, follow these steps:

1. Click **Add Host Connection**.
2. Complete the z/OS host connection details.
3. Click **Import z/OS Connection Certificate** to upload the certificate.
4. When this action is complete, click **Add Host** to create the host connection with the certificate.

   Note: The certificates are automatically synced between the active and standby servers.

Adding a disconnected z/OS host connection

You can import a certificate to add a disconnected z/OS host connection.

To import a certificate for a disconnected z/OS host, follow these steps:

1. Click the disconnected host. This action opens the **View/Modify Host Connection** window.
2. Click **Import z/OS Connection Certificate** to upload the certificate.
3. When this action is complete, click **Update Host** to add the certificate.

   Note: The certificates are automatically synced between the active and standby servers.

Updating a z/OS host connection certificate

You can update the certificate for a z/OS host connection, including when the host is already in a connected state.

To update a z/OS host connection certificate, follow these steps:

1. Click the host. This action opens the **View/Modify Host Connection** window.

   Note: If the host is already connected, all of the fields and controls are disabled except for the **Import z/OS Connection Certificate** button.
2. Click **Import z/OS Connection Certificate** to upload the certificate.
3. When you add another certificate, the **Update Host** button is enabled. Click **Update Host** to add the certificate.

   Note: The certificates are automatically synced between the active and standby servers.

Creating and deploying a policy file for Application Transparent Transport Layer Security

Application Transparent Transport Layer Security (AT-TLS) is a service that is provided by the z/OS Communication Server Policy Agent (PAGENT) and the TCP/IP stack. The AT-TLS service manages connections on behalf of applications that are running on the z/OS operating system. You create the AT-TLS policy file, install the configuration files, and upload them to the necessary z/OS system, for a host connection.

The following steps assume that you have AT-TLS already up and running successfully on your system and the policy agent is configured and activated. See the *IBM z/OS V2R2 Communications Server: IP Configuration Guide* (**SC27-3650-06**) and the *IBM z/OS V2R2 Communications Server: IP Configuration Reference* (**SC27-3651-06**) for more information.

The AT-TLS (`ttlsPol.txt`) policy file is produced by the IBM Configuration Assistant. You can use the IBM Configuration Assistant to create the file and modify it if necessary. You can also modify the one that

was produced by Configuration Assistant with a text editor, or create the file with a text editor. A sample policy file is provided at the end of this task procedure.

The preferred way to create the policy file is to use the IBM Configuration Assistant, or now the IBM z/OS Management Facility (z/OSMF).

Use these steps to create a policy file:

1. Download and install IBM Configuration Assistant for z/OS Communications Server, V1.13 or later.

   You create an AT-TLS policy file by using the Configuration Assistant GUI.

   Note: Starting with z/OS Version 1 Release 1, the IBM Configuration Assistant is replaced by dialogs in the z/OS Management Facility (z/OSMF).

2. Start the configuration assistant by clicking **Start > All Programs > IBM Programs > IBM Configuration Assistant for z/OS > Configuration Assistant V1R13**.

3. From the **Perspective** menu, select **AT-TLS**.

4. In the **AT-TLS Perspective** window, click **Add a New z/OS Image**.

5. In the **New z/OS Image** window, enter information in the **z/OS image name**, **Description**, **z/OS release** and **Key ring** fields, and then click **OK**.

   This key ring name must be the same name that you used when you first generated a key ring. See "Configuring a secure communication between HyperSwap and the client" on page 32.

6. In the **Proceed to the Next Step** window, click **Yes** to add a TCP/IP stack to the z/OS image.

7. In the **New TCP/IP Stack Information** window, type a stack name in the **TCP/IP stack name** field, add information to the **Description** field, and then click **OK**.

8. In the **AT-TLS Perspective** window, click **Add** to create a connectivity rule.

9. In the **New Connectivity Rule** wizard, click **Next**.

10. Identify the data endpoints by completing the following fields:

    a) In the **Connectivity rule name** field, enter a suffix for a name of the rule.

    b) In the **Local data endpoint** field, select **ALL_IP_Addresses**.

    c) In the **Remote data endpoint** field, select **ALL_IP_Addresses**.

    d) Click **Next**.

    A generic rule facilitates testing.

11. Click **Traffic Descriptor**.

12. Click **Add** to add a traffic descriptor.

13. In the **New Traffic Descriptor** page, enter information in the **Name** and **Description** fields. Click **Add**.

    In the **New Traffic Type** notebook, use the **Details** tab to specify the port configuration for the HyperSwap side of the port.

14. In the **New Traffic Type** notebook, click the **Key Ring** tab and specify the certificate label for your key ring and click **OK**. Click **OK** again, and then click **Close**.

15. In the **New Connectivity Rule-Select Requirement Map** page, click **Create a new requirement map**.

    Verify that this new map includes the traffic descriptor that you created in step 12.

    a) In the **Name** field, enter the name of the requirement map.

    b) Click **Security Levels** and add a security level. The security level that you select needs to support TLSv1.2.

    c) Click **Next**.

16. Click **Advanced** to add any other necessary stacks, if not, then click **Finish**.

17. Select the enabled rule from the list and click **Apply Changes**.

18. On the **Image Information** tab, review the pertinent information and click **Application Setup Tasks**.

    Complete the initial setup tasks, including RACF directives and start procedures.

19. In the **Application Setup Tasks** window, click **Display All Instructions** to see more detailed information.

   The **Task Configure Installation Setup** window opens.

20. In the **Task Configure Installation Setup** window, click **Location Information** to input the installation setup.

   The **Installation Location Setup** window opens.

   a) Click **Instructions** to see the documentation that comes bundled with the application.

21. In the **Installation Location Setup** window, enter your correct FTP information to upload the policy file. Click **OK**.

   After the file transfer, refresh or restart the policy agent (PAGENT).

22. In the **AT-TLS Perspective** window, click **Install Configuration Files**.

   The generated policy files are installed for the z/OS image. The **List of Configuration Files** window opens.

23. In an OMVS session, edit the `/etc/pagent/conf.txt` file by adding the following lines:

```
LogLevel=255
CommonTTLSConfig /etc/pagent/ttlsPol.txt
TTLSConfig/etc/pagent/ttlsPol.txt
```

24. In an OMVS session, edit the `/etc/pagent/env.txt` file by adding the following lines:

```
PAGENT_CONFIG_FILE=/etc/pagent/conf.txt
PAGENT_LOG_FILE=/tmp/pagent2.log
```

25. If the member PAGENT does not already exist in `SYS1.PROCLIB`, copy the sample JCL `PAGENT` in the `TCPIP.SEZAINST` library to the system procedure library (for example, `SYS1.PROCLIB`). Then edit the following line in `SYS1.PROCLIB(PAGENT)`:

```
//STDENV    DD PATH='/etc/pagent/env.txt',PATHOPTS=(ORDONLY)
```

26. In the **List of Configuration files** window, view the configuration files and click **Install**.

27. In the **Install Files to Remote host** window, confirm the credentials and the FTP logon information. Verify that the file location is `/etc/pagent/ttlsPol.txt`, and then, click **Go**.

   The policy file is installed.

28. Create a data set, *datasetname* with the following contents:

```
TCPCONFIG TTLS
```

   a) Issue the following command:

```
V TCPIP,TCPIP,OBEYFILE,datasetname
```

29. If PAGENT has not already been started, it needs to be started.

```
START PAGENT
```

30. Then cancel, and restart HSIB.

```
START HSIB
```

The policy file is created and deployed.

Example: AT-TLS policy file

```
##
## AT-TLS Policy Agent Configuration file for:
##     Image: SC30
##     Stack: TCPIP
##
## Created by the IBM Configuration Assistant for z/OS Communications Server
## Version 2 Release 2
## Backing Store = CSM_STORE
```

```
## Install History:
## 2017-01-24 20:40:01 : lascu to 9.12.4.211
##
## End of Configuration Assistant information
TTLSRule                                    HS_test~1
{
LocalAddrSetRef                             addr1
RemoteAddrSetRef                            addr1
LocalPortRangeRef                           portR1
Direction                                   Both
Priority                                    255
TTLSGroupActionRef                          gAct1~Basic_HS
TTLSEnvironmentActionRef                    eAct1~Basic_HS
TTLSConnectionActionRef                     cAct1~Basic_HS
}
TTLSGroupAction                             gAct1~Basic_HS
{
TTLSEnabled                                 On
}
TTLSEnvironmentAction                       eAct1~Basic_HS
{
   HandshakeRole                            Server
   EnvironmentUserInstance                  0
   TTLSKeyringParmsRef                      keyR~SC30
}
TTLSConnectionAction                        cAct1~Basic_HS
{
   HandshakeRole                            Server
   TTLSCipherParmsRef                       cipher1~AT-TLS__Silver
   TTLSConnectionAdvancedParmsRef           cAdv1~Basic_HS
   CtraceClearText                          Off
   Trace                                    2
}
TTLSConnectionAdvancedParms                 cAdv1~Basic_HS
{
TLSv1.2                                     On
HandshakeTimeout                            30
SecondaryMap                                Off
}
TTLSKeyringParms                            keyR~SC30
{
   Keyring                                  csmkeyring
}
TTLSCipherParms                             cipher1~AT-TLS__Silver
{
   V3CipherSuites                           TLS_RSA_WITH_AES_128_CBC_SHA256
   V3CipherSuites                           TLS_RSA_WITH_AES_256_CBC_SHA256
   V3CipherSuites                           TLS_RSA_WITH_AES_128_GCM_SHA256
}
IpAddrSet                                   addr1
{
   Prefix                                   0.0.0.0/0
}
PortRange                                   portR1
{
   Port                                     5858
}
```

Verifying the z/OS system host connection

Use the Copy Services Manager GUI to verify that a host can connect to a z/OS system.

To verify a host connection on the z/OS system, follow these steps:

1. In the Copy Services Manager administrator console, enter your user name and password and click **Log in**.

2. In the **Health Overview** page, click **Host Systems**.

3. In the **Host Systems** page, click **Add Host Connection**.

4. In the **Add Host Connection** dialog, enter the host connection information and click **Add Host**.

   The local host connection is displayed as connected in the list.

Chapter 3. Uninstalling Copy Services Manager

This information guides you through uninstalling Copy Services Manager.

Uninstalling on z/OS

Follow these steps to uninstall Copy Services Manager on a z/OS system.

Recommendation: Before you uninstall Copy Services Manager, be sure to back up data in the current installation with the **mkbackup** command, as described in the IBM Copy Services Manager online product documentation (http://www-01.ibm.com/support/knowledgecenter/SSESK4).

Additionally, review the information on "Backing up and restoring product data," in the *IBM Copy Services Manager User's Guide*. It contains important details about other files and data that you need to back up before you uninstall Copy Services Manager.

A job file can be used to uninstall Copy Services Manager.

Some of the information in the following steps is generic and must be made specific for your particular installation.

1. Use a job file as shown in the following example to remove Copy Services Manager function modification identifiers (FMIDs), Hierarchical File System (HFS) files, and data sets. If you have multiple z/OS systems that are attached to the same driver, you must detach all systems other than the system on which you are uninstalling Copy Services Manager.

```
//REMTPCRM JOB ,'SMP DELETE',REGION=0M,MSGCLASS=H,MSGLEVEL=(1,1),
//  NOTIFY=&SYSUID
//*----------------------------------------------------------
//* The purpose of this job is to DELETE CSM product and
//* its associated datasets.
//* Fill in volser, CSI and HFS dataset names
//*----------------------------------------------------------
//SMPE EXEC  PGM=GIMSMP,REGION=0M      SMP/E EXEC STATEMENT
//SMPLOG DD DUMMY
//SMPOUT   DD  SYSOUT=*
//SMPRPT   DD  SYSOUT=*
//SMPLIST  DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//SMPSNAP  DD  DUMMY
//SMPHOLD  DD  DUMMY
//*SMPTLIB DD  UNIT=3390,VOL=SER=volser,DISP=SHR
//SMPTLIB  DD  UNIT=3390,VOL=SER=VOL,DISP=SHR
//SMPCSI   DD  DSN=HLQ.SMPE.CSI,DISP=OLD  your csi dataset name
//SYSUT1   DD  UNIT=SYSDA,SPACE=(CYL,(200,50)),DISP=(,DELETE)
//SYSUT2   DD  UNIT=SYSDA,SPACE=(CYL,(33,1)),DISP=(,DELETE)
//SYSUT3   DD  UNIT=SYSDA,SPACE=(CYL,(33,1)),DISP=(,DELETE)
//SYSUT4   DD  UNIT=SYSDA,SPACE=(CYL,(33,1)),DISP=(,DELETE)
//SMPWRK1  DD  UNIT=SYSDA,SPACE=(CYL,(25,25,200)),
//             DISP=(,DELETE),DCB=BLKSIZE=6160
//SMPWRK2  DD  UNIT=SYSDA,SPACE=(CYL,(25,25,200)),
//             DISP=(,DELETE),DCB=BLKSIZE=6160
//SMPWRK3  DD  UNIT=SYSDA,SPACE=(CYL,(90,45,2000)),
//             DISP=(,DELETE),DCB=BLKSIZE=3200
//SMPWRK4  DD  UNIT=SYSDA,SPACE=(CYL,(25,25,500)),
//             DISP=(,DELETE),DCB=BLKSIZE=3200
//SMPWRK6  DD  UNIT=SYSDA,SPACE=(CYL,(200,75,2000)),
//             DISP=(,DELETE),DCB=BLKSIZE=6160
//SMPPTFIN DD *
++FUNCTION(DELPROD) .
++VER(Z038)

DELETE(HIWN62H,JIWN62X).
/*
//SMPCNTL DD *
  SET BDY(GLOBAL) .
  RECEIVE LIST SYSMODS .
  SET BDY(RMTZN) .
  APPLY S(DELPROD) BYPASS(ID) C(ALL) .
  SET BDY(RMDZN) .
```

```
    ACCEPT S(DELPROD) C(ALL) .
    SET BDY(RMTZN) .
    UCLIN .
    DEL SYSMOD(DELPROD) .
    ENDUCL .
    SET BDY(RMDZN) .
    UCLIN .
    DEL SYSMOD(DELPROD) .
    ENDUCL .
    SET BDY(GLOBAL) .

  REJECT DELETEFMID(HIWN62H) NOFMID .
    REJECT DELETEFMID(JIWN62X) NOFMID .
    LIST ALLZONES FORFMID(HIWN62H) .
    LIST ALLZONES FORFMID(JIWN62X) .
  /*
//*
//*----- This step will unmount HFS datasets associated with CSM
//*
//UNMOUNT EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
    PROFILE WTPMSG MSGID
    TIME
    UNMOUNT FILESYSTEM('<CSM_InstallRoot>') IMMEDIATE
    UNMOUNT FILESYSTEM('<CSM_ProductionRoot>') IMMEDIATE
/*
//DELETE EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *

DELETE    CSM.AIWNHFS.SYSD
  DELETE CSM.AIXNHFS2.SYSD
  DELETE    CSM.AIWNHFSX.SYSD
  DELETE    CSM.ASAMPLIB.SYSD
  DELETE    CSM.SAMPLIB.SYSD
  DELETE    <CSM_InstallRoot>
  DELETE    <CSM_ProductionRoot>
/*                                  */
/*  DELETE ALL SMPE DATASETS        */
/*                                  */
  DELETE    HLQ.SMPE.CSI CLUSTER
  DELETE    HLQ.SMPE.GLOBAL.SMPLOG
  DELETE    HLQ.SMPE.GLOBAL.SMPLOGA
  DELETE    HLQ.SMPE.RMDZN.SMPLOG
  DELETE    HLQ.SMPE.RMDZN.SMPLOGA
  DELETE    HLQ.SMPE.RMTZN.SMPLOG
  DELETE    HLQ.SMPE.RMTZN.SMPLOGA
  DELETE    HLQ.SMPE.SMPLTS
  DELETE    HLQ.SMPE.SMPMTS
  DELETE    HLQ.SMPE.SMPPTS
  DELETE    HLQ.SMPE.SMPSTS
  DELETE    HLQ.SMPE.SMPSCDS//
```

2. Ensure that WebSphere® Application Server for z/OS Liberty Profile is in the stop state. For instructions for stopping WebSphere Application Server for z/OS Liberty Profile, see "Configuring the IWNSRV job" on page 21.

Uninstalling on distributed systems

Follow these steps to uninstall Copy Services Manager on distributed systems.

Recommendation: Before you uninstall Copy Services Manager, be sure to back up data in the current installation with the **mkbackup** command, as described in the IBM Copy Services Manager online product documentation (http://www-01.ibm.com/support/knowledgecenter/SSESK4).

Additionally, review the information on "Backing up and restoring product data," in the *IBM Copy Services Manager User's Guide*. It contains important details about other files and data that you need to back up before you uninstall Copy Services Manager.

Follow this process to uninstall Copy Services Manager:

- Click the shortcut, **Uninstall**, that is in the CSM installation directory at:

Option	Description
Windows	`C:/Program Files/IBM/CSM/Uninstall`
Linux/AIX	`/opt/IBM/CSM/Uninstall`

- The shortcut points to the uninstall executable file in the `UninstallData` directory.

  Note: The Copy Services Manager uninstaller gives you the option to either completely remove all features and components, or to leave configuration files and logs in place. If you plan to reinstall Copy Services Manager, it is suggested that you choose the option to leave these files in place. They retain user authentication data to help you get set up again faster.

- Alternatively, you can uninstall Copy Services Manager with the program-removal function that is available on the operating system on which it was installed. For example, on Windows, you can uninstall Copy Services Manager from the **Start** menu (**Start** > **All Programs** > **IBM Copy Services Manager** > **Uninstall IBM Copy Services Manager**), or from the Programs category in the Control Panel.

Chapter 4. Migrating Copy Services Manager

You can migrate from an existing installation of Tivoli Storage Productivity Center for Replication, version 5.2.0 or later, to Copy Services Manager with the installation setup file.

Migrating on z/OS

Migrate Copy Services Manager on z/OS by running the installation setup file that is provided with your license.

Migrating from Tivoli Storage Productivity Center for Replication to Copy Services Manager

If you are migrating from Tivoli Storage Productivity Center for Replication to Copy Services Manager, first follow these steps:

1. Open the `rmserver.properties` file and ensure that it can be viewed in an Interactive System Productivity Facility (ISPF) editor. You can locate this file at: `<Production_root>/opt/Tivoli/RM/wlp/usr/servers/replicationServer/properties/rmserver.properties`

   - If you can view the file in an ISPF editor, then no further action is needed. You can continue to the migration procedure.
   - If the file cannot be viewed, it is because Tivoli Storage Productivity Center for Replication used ASCII instead of EBCDIC encoding. Proceed to step 2.

2. Download the file in binary format to your local desktop.
3. Create a backup of the file on the z/OS system.
4. Open the `rmserver.properties` file in a text editor.
5. Edit the `rmserver.properties` file on z/OS in an ISPF editor, and delete all of the contents.
6. Replace all of the contents by using copy and paste from the downloaded file.
7. Save the file on the system.
8. Continue to the migration procedure.

To migrate from Tivoli Storage Productivity Center for Replication to Copy Services Manager on z/OS, see "Installing on IBM Z" on page 5.

The following value can be used in the IWNINSTL script for migrating:

```
MIGRATION_FROM=path_prefix/opt/Tivoli/RM
```

MIGRATION_FROM
Specifies the location of the Tivoli Storage Productivity Center for Replication database to be used for the migration.

Migrating on distributed systems

Migrate to Copy Services Manager on distributed systems by running the installation setup file that is provided with your license.

You need to issue the **mkbackup** command on the existing Tivoli Storage Productivity Center for Replication or Copy Services Manager server before you start the migration. The name of the compressed (`.zip`) file that is created by the **mkbackup** command is used during the migration to identify the path to the backup archive file. The Copy Services Manager migration function uses the information in the backup file to load in all storage system connections, session configurations, and so on.

For more information on the **mkbackup** command, see the IBM Copy Services Manager online product documentation (http://www-01.ibm.com/support/knowledgecenter/SSESK4).

Starting with Copy Services Manager version 6.1.2, you can also use the GUI to issue a backup. In the Copy Services Manager GUI, go to **Settings** > **Advanced Tools**, and find the **Create Backup** section to proceed.

The following steps are used to migrate from Tivoli Storage Productivity Center for Replication to Copy Services Manager, or to migrate from one Copy Services Manager server to another.

1. Run the installation setup file.

   Silent migration: You can also migrate by using the silent installation, by inserting CSM_BACKUP in the response file. See "Silent installation" on page 24 for details.

2. On the **Choose Installation Method** page, select **Migrate/Restore using existing backup**.

3. Identify the path to the backup archive file that is created by the **mkbackup** command, or by creating the backup file from the GUI.

4. Click **Validate** to verify that the selected backup archive file is valid.

5. Click **Next** to enter other installation details and complete the migration to Copy Services Manager.

Chapter 5. Upgrading Copy Services Manager

Use the information in this topic to upgrade from Tivoli Storage Productivity Center for Replication to Copy Services Manager, or from one version of Copy Services Manager to another.

Important: It is suggested that you first back up your Tivoli Storage Productivity Center for Replication database before you proceed with an upgrade from Tivoli Storage Productivity Center for Replication to Copy Services Manager. Create the backup database by using the **mkbackup** command on the Tivoli Storage Productivity Center for Replication CLI.

Upgrading on z/OS

You can upgrade from Tivoli Storage Productivity Center for Replication to Copy Services Manager on z/OS, or you can upgrade Copy Services Manager from a different version.

Upgrading from Tivoli Storage Productivity Center for Replication to Copy Services Manager

During the upgrade, the Tivoli Storage Productivity Center for Replication management server is not available. Therefore, the capability for disaster recovery during the upgrade process is not available unless you establish a high-availability environment. A high-availability environment includes an active and standby management server.

See your Tivoli Storage Productivity Center for Replication product documentation for instructions on how to set up a standby management server if you do not have one already.

If you want to maintain disaster recovery capability, you must complete the steps to perform a takeover on the standby management server before you upgrade the active management server. The standby management server continues to manage sessions during the upgrade process, which ensures disaster recovery capability and minimizes downtime if the upgrade fails.

If you do not want to maintain disaster recovery capability during the migration process, a standby management server is not required. In general, this migration method is used only if you are using Tivoli Storage Productivity Center for Replication only for monitoring purposes and are not managing sessions. If you use this method, it is more difficult to restore your Tivoli Storage Productivity Center for Replication configuration if the upgrade fails.

Note: When you upgrade from Tivoli Storage Productivity Center for Replication to Copy Services Manager, the port assignments are not preserved unless you set them in IWNINSTL before the upgrade. For more information, see .

To upgrade from Tivoli Storage Productivity Center for Replication to Copy Services Manager on z/OS, ensure that all Copy Services Manager installation and postinstallation tasks are complete. When you run the IWNINSTL script, all optional values can be updated, including port assignments and the time zone designation. There are two new values in the IWNINSTL script for this type of upgrade:

TPCR_ProductionRoot=path_prefix/opt/Tivoli/RM
Specifies the production root that was used when Tivoli Storage Productivity Center for Replication was installed. Update this path to indicate what directory path for Copy Services Manager to use for the upgrade.

KEEP_TPCR (optional) TRUE/FALSE
Default is KEEP_TPCR=false. If set to true, when you upgrade from Tivoli Storage Productivity Center for Replication to Copy Services Manager, the TPCR directory structure is not deleted.

After you process the IWNINSTL script, and you start IWNSRV and IWNAUTH, Copy Services Manager is accessible at: *https://<host name>:<GUI_PORT>/CSM/*

To upgrade from Tivoli Storage Productivity Center for Replication to Copy Services Manager while you maintain disaster recovery capability, complete all of the following steps. To upgrade without maintaining

disaster recovery capability, complete steps .

1. Verify that the synchronization of the standby server is complete and that the Tivoli Storage Productivity Center for Replication sessions are not in a transitory state, such as Preparing, Suspending, or Recovering.

2. Move the management of the Tivoli Storage Productivity Center for Replication on the secondary server by issuing the **Takeover** command.

3. On the primary server, remove the secondary standby server from the HA relationship definition. The active Tivoli Storage Productivity Center for Replication on the secondary server continues to manage sessions during the upgrade process on the primary server.

4. Stop Tivoli Storage Productivity Center for Replication on the primary server.

5. Install Copy Services Manager Version 6.1 or later on the primary server by using the SMP/E tool for installing and maintaining software on z/OS systems.

   Note: For more information, see the *IBM Program Directory for Copy Services Manager for z Systems* or the *IBM Program Directory for Copy Services Manager Basic Edition for z Systems*. For more information on how to locate these directories, see .

6. Complete the postinstallation steps for z/OS after you install IBM Copy Services Manager. Before you run the IWNINSTL script, update it to use the value TPCR_ProductionRoot (optionally use KEEP_TPCR). For more information, see .

7. When the sessions are not in a transitory state, start Copy Services Manager on the primary server. Verify that it shows all sessions in the same state as they were before the upgrade.

8. Repeat steps through that were completed on the primary server, but now perform them on the secondary server.

9. Reestablish the high availability (HA) relationship that was originally set up between the primary and secondary servers.

When all of these tasks are finished, the upgrade from Tivoli Storage Productivity Center for Replication to Copy Services Manager is complete.

Upgrading from a different version of Copy Services Manager

During the upgrade, the Copy Services Manager management server is not available. Therefore, the capability for disaster recovery during the migration process is not available unless you establish a high-availability environment. A high-availability environment includes an active and standby management server.

If you want to maintain disaster recovery capability, you must complete the steps to perform a takeover on the standby management server before you upgrade the active management server. The standby management server continues to manage sessions during the upgrade process, which ensures disaster recovery capability and minimizes downtime if the upgrade fails.

For more information on setting up a standby management server, see the *IBM Copy Services Manager User's Guide* chapter titled "Managing management servers." See for instructions on where to locate this guide.

If you do not want to maintain disaster recovery capability during the migration process, a standby management server is not required. In general, this migration method is used only if you are using Copy Services Manager only for monitoring purposes and are not managing sessions. If you use this method, it is more difficult to restore your Copy Services Manager configuration if the upgrade fails.

Note: When you upgrade to a newer version of Copy Services Manager, the port assignments are preserved as they were before the upgrade.

To upgrade Copy Services Manager on z/OS while you maintain disaster recovery capability, complete all of the following steps. To upgrade without maintaining disaster recovery capability, complete steps .

1. Verify that the synchronization of the standby server is complete and that the Copy Services Manager sessions are not in a transitory state such as Preparing, Suspending, or Recovering.
2. Move the management of the Copy Services Manager to the standby on the secondary server by issuing the **Takeover** command.
3. On the primary server, remove the secondary standby server from the HA relationship definition. The active Copy Services Manager on the secondary server continues to manage sessions during the upgrade process on the primary server.
4. Stop Copy Services Manager on the primary server.
5. Upgrade the primary server to Copy Services Manager Version 6.1 or later by using the SMP/E tool for installing and maintaining software on z/OS systems.

   Note: For more information, see the *IBM Program Directory for Copy Services Manager for z Systems* or the *IBM Program Directory for Copy Services Manager Basic Edition for z Systems*. For more information on how to locate these directories, see "Publications and related information" on page viii.
6. Run the IWNINSTL job again to complete the upgrade on the primary server. For more information, see "Configuring the IWNINSTL job" on page 18.

   Note: For information on other postinstallation steps for z/OS after Copy Services Manager is installed or upgraded, see "Postinstallation tasks for IBM Z" on page 5. The only postinstallation step that is required for an upgrade is IWNINSTL. The other steps were run for the previous installation. However, if you want to change your RACF configuration, then you can update and run the RACF jobs.
7. When the sessions are not in a transitory state, start Copy Services Manager on the primary server. Verify that it shows all sessions in the same state as they were before the upgrade.
8. Repeat steps "4" on page 45 through "7" on page 45 that were completed on the primary server, but now perform them on the secondary server.
9. Reestablish the high availability (HA) relationship that was originally set up between the primary and secondary servers.

When all tasks are finished, the upgrade from a previous version of Copy Services Manager is complete.

Upgrading on distributed systems

You can upgrade Copy Services Manager to a different version by running the latest installation setup file.

During the upgrade, the Copy Services Manager management server is not available. Therefore, the capability for disaster recovery during the upgrade process is not available unless you establish a high-availability environment. A high-availability environment includes an active and standby management server.

If you want to maintain disaster recovery capability, you must complete the steps to perform a takeover on the standby management server before you upgrade the active management server. The standby management server continues to manage sessions during the upgrade process, which ensures disaster recovery capability and minimizes downtime if the upgrade fails.

For more information on setting up a standby management server, see the *IBM Copy Services Manager User's Guide* chapter titled "Managing management servers." See "Publications and related information" on page viii for instructions on where to locate this guide.

If you do not want to maintain disaster recovery capability during the migration process, a standby management server is not required. In general, this migration method is used only if you are using Copy Services Manager only for monitoring purposes and are not managing sessions. If you use this method, it is more difficult to restore your Copy Services Manager configuration if the upgrade fails.

Note: When you upgrade to a newer version of Copy Services Manager, the port assignments are preserved as they were before the upgrade.

To upgrade Copy Services Manager on a distributed system while you maintain disaster recovery capability, complete all of the following steps. To upgrade without maintaining disaster recovery capability, complete steps "4" on page 46, "5" on page 46, "6" on page 46, and "7" on page 46.

1. Verify that the synchronization of the standby server is complete and that the Copy Services Manager sessions are not in a transitory state such as Preparing, Suspending, or Recovering.
2. Move the management of the Copy Services Manager to the secondary server by issuing the **Takeover** command while it has the standby role. After the takeover, the primary server is removed and Copy Services Manager on the secondary server has an active role.
3. On the primary server, remove the secondary standby server from the HA relationship definition. The active Copy Services Manager on the secondary server continues to manage sessions during the upgrade process on the primary server.
4. On the primary server, run the installation setup file for the version to which you are upgrading.

   Note: During an upgrade of Copy Services Manager, you are not presented with the **Select Installation Type** page that is displayed during an initial installation, or a migration or restoration from a backup.
5. The **Upgrade IBM Copy Services Manager** page displays the currently installed version and the version that you will upgrade to. Click **Next** to continue the upgrade.
6. On the **Software License Agreement** page, agree to the terms and click **Next**.
7. The **Pre-installation Summary** page is displayed. Click **Next** to complete the upgrade on the primary server.
8. Verify that the upgraded primary server restarted Copy Services Manager in the new version, and that it shows all sessions in the same state as they were before the upgrade.
9. Repeat steps "4" on page 46 through "7" on page 46 that were completed on the primary server, but now perform them on the secondary server.
10. Reestablish the high availability (HA) relationship that was originally set up between the primary and secondary servers.

When all tasks are finished, the upgrade from a previous version of Copy Services Manager is complete.

Upgrading on a DS8000 HMC

You can install or upgrade Copy Services Manager on a DS8000 HMC by using the DSCLI.

For instructions on installing or upgrading Copy Services Manager on a DS8000 Hardware Management Console (HMC), see the DS8000 command-line (DSCLI) help information for the **lssoftware** and **installsoftware** commands in the online help documentation at http://www.ibm.com/support/knowledgecenter/ST5GLJ/ds8000_kcwelcome.html.

Chapter 6. Using Copy Services Manager on the DS8000

This information covers tasks that are specific to using Copy Services Manager for DS8000.

Exporting the Copy Services Manager license from the DS8000 HMC to run on a separate server

You can export the Copy Services Manager license from the DS8000 HMC to run on a separate server.

To export the Copy Services Manager license from the HMC, you must first export either a license (`.zip`) file, or a license key string, and then update the license.

1. Follow the procedure in "Exporting a license file" on page 25 to export a license (`.zip`) file. Or follow the procedure in "Copying a license key" on page 25 to export a license key string.
2. Follow the procedure in "Applying license files after installation or migration, or updating licenses" on page 26.

The Copy Services Manager license is exported from the DS8000 HMC to run on a separate server.

Exporting a license from a stand-alone Copy Services Manager server and importing to the DS8000 HMC

You can export a license from a stand-alone Copy Services Manager server and import it to a DS8000 HMC.

To export the Copy Services Manager license from a stand-alone Copy Services Manager server to import it to a DS8000 HMC, you must first copy a license key string, and then update the license.

1. Follow the procedure in "Copying a license key" on page 25.
2. Follow the procedure in "Applying license files after installation or migration, or updating licenses" on page 26.

The Copy Services Manager license is exported from a stand-alone Copy Services Manager server and imported to a DS8000 HMC.

Getting Copy Services Manager code updates onto the DS8000 HMC by using DSCLI commands

You can obtain Copy Services Manager code updates for the DS8000 HMC by using the **lssoftware** and **installsoftware** DSCLI commands.

DSCLI commands are available for obtaining Copy Services Manager code updates for the DS8000 HMC.

1. Follow the procedure in "Upgrading on a DS8000 HMC" on page 46 to locate the DSCLI command help information.
2. Locate and follow the command help for the **lssoftware** DSCLI command.
3. Locate and follow the command help for the **installsoftware** DSCLI command.

Copy Services Manager code is updated for the DS8000 HMC.

Converting a license file to a string key for Copy Services Manager enablement on the DS8000 HMC

You can enable Copy Services Manager for use on a DS8000 HMC by converting the license file to a string key.

If you only have a stand-alone Copy Services Manager license file (`csm-license.zip`), then you need to convert that file to a string key to enable the DS8000 HMC. The HMC only accepts a string key for enablement.

You can convert the file to a string key by using either a GUI interface, or the silent installation method.

Converting a license file to a string key for Copy Services Manager enablement on the DS8000 HMC by using a GUI

You can choose to convert the license file by using an installation wizard that you download from Fix Central.

Follow these steps to convert the `csm-license.zip` license file to a string key to use for HMC enablement by using a GUI:

1. Go to IBM Fix Central (www.ibm.com/support/fixcentral), search under Copy Services Manager, and download the Install File that is associated with your operating system.
2. Open a command line.
3. Change directories to where the `setup.exe` file is located. Or, you can point to the relevant directory.
4. Enter the following command:
   ```
   cmd /c copy_services_manager_setup.exe -DCSM_GENERATE_KEY=true
   For example:
   cmd /c csm-setup-6.1.x-win.exe -DCSM_GENERATE_KEY=true
   ```
5. Browse from within the Copy Services Manager Install File (installation wizard) to select the `csm-license.zip` file.
6. Click **Generate** to convert the file to a string key.

   Note: If you receive an error message that your license file is not valid, contact IBM Support.
7. When you are done, click **Next** to quit and exit, or click **Cancel** to exit without saving any changes.

The Copy Services Manager string key is generated to use for enablement on a DS8000 HMC.

Converting a license file to a string key for Copy Services Manager enablement on the DS8000 HMC by using a silent installation method

You can choose to convert the license file by using the silent installation method.

Follow these steps to convert the `csm-license.zip` license file to a string key to use for HMC enablement by using the silent installation method:

1. Open a command line.
2. Change directories to where the `setup.exe` file is located. Or, you can point to the relevant directory.
3. Enter the following command:
   ```
   cmd /c copy_services_manager_setup.exe -i silent -DLICENSE_ACCEPTED=true -
   DCSM_GENERATE_KEY=true -DCSM_LICENSE_FILE=/home/csmadmin/csm-license.zip
   For example:
   cmd /c csm-setup-6.1.x-win.exe -i silent -DLICENSE_ACCEPTED=true -
   DCSM_GENERATE_KEY=true -DCSM_LICENSE_FILE=/home/csmadmin/csm-license.zip
   ```

The Copy Services Manager string key is generated to use for enablement on a DS8000 HMC.

Appendix A. Configuration files

This topic provides default file locations for Copy Services Manager configuration files.

The following table shows the default file location for each configuration file.

Configuration file	Default location
`bootstrap.properties`	• For management server on distributed systems: *install dir*`\liberty\wlp\usr\servers\csmServer\bootstrap.properties` • For authentication server on distributed systems: *install dir*`\liberty\wlp\usr\servers\csmAuth\bootstrap.properties` • For management server on z/OS: *path_prefix*`/opt/IBM/CSM/wlp/usr/servers/csmServer/bootstrap.properties` • For authentication server on z/OS: *path_prefix*`/opt/IBM/CSM/wlp/usr/servers/csmAuth/bootstrap.properties`
`csmConnections.properties`	• For distributed systems: *install dir*`\liberty\wlp\usr\servers\csmServer\properties` • For z/OS: *path_prefix*`/opt/IBM/CSM/wlp/usr/servers/csmServer/properties`
`diagnostics.properties`	• For distributed systems: *install dir*`\liberty\wlp\usr\servers\csmServer\properties` • For z/OS: *path_prefix*`/opt/IBM/CSM/wlp/usr/servers/csmServer/properties`
`repcli.properties`	• For distributed systems: *install dir*`\CLI` • For z/OS: *path_prefix*`/opt/IBM/CSM/CLI`
`rmserver.properties`	• For distributed systems: *install dir*`\liberty\wlp\usr\servers\csmServer\properties` • For z/OS: *path_prefix*`/opt/IBM/CSM/wlp/usr/servers/csmServer/properties`

bootstrap.properties file

Two `bootstrap.properties` files contain the configuration attributes for the Copy Services Manager servers. One bootstrap properties file sets the configuration for the management server and another for the authentication server.

The `bootstrap.properties` file is in the following locations on distributed systems:

- Management server: *install_dir*`\liberty\wlp\usr\servers\csmServer\bootstrap.properties`
- Authentication server: *install_dir*`\liberty\wlp\usr\servers\csmAuth\bootstrap.properties`

The `bootstrap.properties` file is in the following locations on z/OS systems:

- Management server: *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/
  bootstrap.properties
- Authentication server: *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmAuth/
  bootstrap.properties

.

The file contains the following properties:

https_port_var
> Specifies the GUI port (for csmServer) or the authentication port (for csmAuth). The port number is set during installation. However, you can modify this property value to change the port number after installation.

keystore_id
> Specifies a unique configuration ID.

keystore_location_prefix
> Simplifies specification of the key ring URL for z/OS. The default value is blank for file-based keystores.

keystore_location
> Specifies an absolute or relative path to the keystore file. If a relative path is provided (for example, key.jks), the server attempts to locate the file in the csmServer/resources/security directory.

keystore_password
> Specifies the password that is used to load the keystore file. The value can be stored in cleartext or encoded form. An encoded password string is preceded with {xor}.

keystore_type
> Specifies a keystore type that is supported by the target SDK. The default value is JKS.

keystore_fileBased
> Specifies whether the keystore is based on a file. The default value is true.

keystore_readOnly
> Specifies whether the keystore is to be used by the server for read operations only. The default value is false. The value false indicates that the server can write to the keystore.

ssl_protocol
> Specifies the SSL handshake protocol that is used on the HTTPS port for that server. The value is determined by the Java release and can default to the minimum value (for instance, TLSv1.2) automatically during upgrade.

Note: You must restart the server for your modifications of the bootstrap properties file to take effect in the server configuration.

The default contents of each bootstrap.properties file is displayed in the following example.

```
################################################################################
#This section is for the HTTPS settings of the IBM Copy Services Manager GUI. #
################################################################################
https_port_var=9559
ssl_protocol=TLSv1.2

################################################################################
#This section is for the keystore certificate information.  This can be       #
#changed to match your environment.                                           #
#                                                                             #
#Note that keystore_location is relative to csmServer/resources/security      #
#The keystore_location_prefix is typically left blank for file based          #
#keystores.                                                                   #
################################################################################
keystore_id=keystore
keystore_location_prefix=
keystore_location=key.jks
keystore_password={xor}HjktbwhvMzkMOi0pOi0=
keystore_type=JKS
keystore_fileBased=true
keystore_readOnly=false
```

```
#######################################################################
#This section is a sample JCERACFKS certificate keystore configuration that  #
#can be uncommented and modified to match your environment.                   #
#                                                                             #
#The location must be a safkeyring url syntax with the first qualifier as the #
#IWNSRV and keyring owner and the second qualifier as the keyring name.  The  #
#safkeyring url syntax is important, in order to pass it properly into        #
#server.xml, it is split across two properties values.  The                   #
#keystore_location_prefix is set to "safkeyring:" while the keystore_location #
#is the rest of the safkeyring url.                                           #
#                                                                             #
#The keystore id and password will be used to create a local keystore with   #
#the specified ID and password holding the cached certificate for the GUI.    #
#######################################################################
#keystore_id=keystore
#keystore_location_prefix=safkeyring:
#keystore_location=//CSMUSER/GUIKEYRING
#keystore_password=password
#keystore_type=JCERACFKS
#keystore_fileBased=false
#keystore_readOnly=true
```

csmConnections.properties file

The csmConnections.properties file contains configuration information about Copy Services Manager graphical user interface (GUI) and management server connection information.

The csmConnections.properties file is located in the *install dir*\liberty\wlp\usr\servers\csmServer\properties directory on distributed systems, and the *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/properties directory on z/OS.

The file contains the following properties:

csm.server.address
> The domain name or IP address of the Copy Services Manager server. The default value is localhost.
>
> **Tip:** This value must match the value of the **server** property in the *install dir*\CLI\repcli.properties file on distributed systems, and the *path_prefix*/opt/IBM/CSM/CLI/repcli.properties file on z/OS.

csm.server.port
> The client port for the GUI to connect to the management server. The default value is 9560.
>
> **Tip:** This value must match the *install dir*\liberty\wlp\usr\servers\csmServer\properties\rmserver.properties file and the **port** property in the *install dir*\CLI\repcli.properties file on distributed systems; and the *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/properties/rmserver.properties file, and the **port** property in the *path_prefix*/opt/IBM/CSM/CLI/repcli.properties file on z/OS.

csm.server.authtype
> The authentication type for the GUI to connect to the management server. The default value is certificate.

csm.server.keystore
> The location of the csmGuiTrust trust file for certificate authentication of the GUI. The default value is /etc.

csm.server.certificate
> The certificate ID. The default value is csmserverdefault.

csm.server.standbyPort
> The HTTPS port that is used for a standby management server. Define this property if the active and standby management servers run on two different GUI ports to ensure that the URL links to the other management server are valid. For example, if you have an active Windows management server that uses port 9559 for the GUI and a standby z/OS management server that uses port 33209 for the GUI, set this property, if you want the GUIs to be able to start the remote GUI.

The default contents of each `csmConnections.properties` file is displayed in the following example.

Note: The values that are set in this file are case-sensitive and must not contain spaces.

```
#
# Define the information for connecting to the CSM Server.
#
csm.server.address=localhost
csm.server.port=9560


#######################################################################
# CERTIFICATE BASED AUTHENTICATION FROM UI TO CSM SERVER
#######################################################################
csm.server.authtype=certificate
csm.server.keystore=etc/csmTrust.jks
csm.server.certificate=csmserverdefault

#csm.server.standbyPort=
```

diagnostics.properties file

The `diagnostics.properties` file contains configuration information about Copy Services Manager log packages.

The `diagnostics.properties` file is in the *install dir*\liberty\wlp\usr\servers \csmServer\properties directory on distributed systems, and the *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/properties directory on z/OS.

Restart the Copy Services Manager graphical user interface to activate property changes. Properties are not synchronized between the Copy Services Manager management servers and must be maintained on each Copy Services Manager management server.

The file contains the following properties:

sourcedir
　　The source directory to be used to create the Copy Services Manager log package.

targetdir
　　The target directory where Copy Services Manager log packages are to be created. The default directory is *install dir*\liberty\wlp\usr\servers\csmServer\diagnostics on distributed systems, and *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/ diagnostics on z/OS.

repcli.properties file

The `repcli.properties` file contains the server and port information that is used to communicate with the Copy Services Manager server and the command-line interface.

The `repcli.properties` file is located in the *install dir*\CLI\ directory for distributed systems, and the *path_prefix*/opt/IBM/CSM/CLI directory for z/OS.

Restart Copy Services Manager to activate property changes. Properties are not synchronized between the Copy Services Manager management servers and must be maintained on each Copy Services Manager management server.

The file contains the following properties:

server
　　The domain name or IP address of the Copy Services Manager server. The default value is `localhost`.

　　Tip: This value must match the value of the **csm.server.address** property in the *install dir* \liberty\wlp\usr\servers\csmServer\csmConnections.properties file for distributed

systems, and the *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/
`csmConnections.properties` file for z/OS.

port
The client port that is used by the CLI to communicate with the Copy Services Manager server. The default value is 9560.

Tip: This value must match the **communications.port** property in the `rmserver.properties` file that is located in the *install dir*\liberty\wlp\usr\servers\csmServer\ directory for distributed systems, and in the *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/ directory for z/OS. And this value must also match the **csm.server.port property** in the `csmConnections.properties` file in the *install dir*\liberty\wlp\usr\servers \csmServer\ directory for distributed systems, and the *path_prefix*/opt/IBM/CSM/wlp/usr/ servers/csmServer/ directory for z/OS.

`rmserver.properties` file

The `rmserver.properties` file contains various configuration settings for Copy Services Manager server.

The default location of the `rmserver.properties` file is the *install dir*\liberty\wlp\usr \servers\csmServer\properties directory on distributed systems, and the *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/properties directory on z/OS.

Note: You can use the **chsystem** command with the **-f server** parameter to change the properties.

Restart Copy Services Manager to activate the property changes. Properties are not synchronized between the Copy Services Manager management servers and must be maintained on each Copy Services Manager management server.

The file contains the following parameters that you might need to customize for your environment:

log.file
The name of the Copy Services Manager server log file. The default value is `csmTrace.log`.

The newest log file is the name the same as this value. Subsequent log files have a number that is appended to the file name. For example, `csmTrace1.log` and `csmTrace2.log`.

This log file is in the *install dir*\liberty\wlp\usr\servers\csmServer\logs\CSM directory on distributed systems, and the *path_prefix*/opt/IBM/CSM/wlp/usr/servers/ csmServer/logs/CSM directory on z/OS.

log.file.maxFiles
The maximum number of Copy Services Manager server log files that are created before old log files are overwritten. The default value is 50.

log.file.maxFileSize
The maximum size, in KB, of each Copy Services Manager server log file. The default value is 10240.

communications.port
The client port that is used by the GUI and CLI to communicate with the Copy Services Manager server. The default value is 9560.

Tip: This value must match the **port** property in the *install dir*\CLI\repcli.properties file and the *install dir*\libery\wlp\usr\servers\csmServer\properties \csm.Connection.properties file on distributed systems; and it must match the **port** property in the *path_prefix*/opt/IBM/CSM/CLI/repcli.properties file and the *path_prefix*/opt/IBM/CSM/wlp/usr/servers/csmServer/properties/ csmConnection.properties file on z/OS.

communications.haPort
The standby management server port that is used for communication between the active and standby management server. The default value is 9561.

csm.server.snmp_community_string
The SNMP community name. The default value is `public`.

csm.server.sus_gc_pairs_on_gm_pause
A flag that indicates whether to suspend the Global Copy pairs when a Global Mirror session is suspended. The valid values are `true` and `false`.

db.backup.location
The directory that is used by the `mkbackup` command to store a backup copy of the IBM Copy Services Manager database. By default, the backup file is stored in the *install dir*`\liberty\wlp\usr\servers\csmServer\database\csmdb` directory for distributed systems, or in the *path_prefix*`/opt/IBM/CSM/wlp/usr/servers/csmServer/database/csmdb` directory for z/OS.

server.logpackages.maxpackages
The maximum number of log packages that is maintained by the server.

server.backup.maxbackups
The maximum number of backups that is maintained by the server.

csm.server.notification.sender.address: *<email address>*
Specifies the email address from which to send outgoing email alerts. By default, outgoing email alerts are set to come from the generated email address csmServer@*<server hostname>*. However, for some SMTP server software or configurations, this email address is not accepted. Therefore, you can change the outgoing server email address to something that meets the requirements of your environment.

csm.server.ldap.enabled
Enables LDAP in your environment when set to `true`.

> **Note:** The default value for **csm.server.ldap.enabled** is set to `false` for z/OS systems and `true` for distributed systems.

com.ibm.csm.*<sessionName>***.***<rolepair>***.userpfc**
Specifies which of the Metro Mirror relationships for the Preserve Mirror feature to use. When the Metro Mirror pairs are established, any pairs that are marked with this property are set up so that when the source is flashed the Preserve Mirror feature knows to use these pairs. For example, setting the property to `com.ibm.csm.MySess.H1-H2.userpfc` indicates that session "MySess" and the role pair "H1-H2" should be used for Preserve Mirror.

> **Notes:**
>
> - This property default is set to `false`. It must be set to `true` to enable the option on the role pair.
> - Use underscores to indicate any spaces in the property setting. For example, for the session "My Sess" you would specify `My_Sess` in the property.
>
> .

com.server.svc.fc.cleanreate =*<cleanrate>*
com.server.svc.fc.cleanrate.*<sessionName>***=***<cleanrate>*
A cleaning rate can be specified for a FlashCopy session (or a session that contains a FlashCopy sequence) that is independent of the background copy rate. The clean rate controls the rate at which the cleaning process operates. The cleaning process copies data from the target volume of a mapping to the target volumes of other mappings that depend on this data.

> **Notes:**
>
> - For older storage systems running IBM Spectrum Virtualize, the *<cleanrate>* range is 0-100. For new storage systems at release 7.8.1 and higher, the range is 0-150. If this property is not specified, the default rate is 50. For more information on the clean rate, see your storage system user's guide.
> - This property is only valid for storage systems running IBM Spectrum Virtualize. If a *<sessionName>* is not specified, the cleaning rate value is applied to all FlashCopy sessions, and sessions that contain a FlashCopy sequence, for storage systems running IBM Spectrum Virtualize.

csm.auto.restart.after.swap=*<true>*

> After a swap occurs, this option automatically restarts replication from the site that was swapped to, to the alternative site without user intervention.
>
> When HyperSwap is enabled on multi-target sessions with Metro Mirror relationships, by default a HyperSwap command or event results in all I/O being swapped to the Metro Mirror secondary. And then the Copy Services Manager session moves to a Target Available state.
>
> After the swap, no replication occurs, and a manual **Start** command must be issued for replication to run again.
>
> If HyperSwap is enabled on the role pair that is automatically started, as soon as all pairs in the role pair reach a Prepared state, the HyperSwap configuration is automatically loaded as well. This option helps to ensure that replication is started quickly after a HyperSwap command or event to provide continual disaster recovery and high availability needs.
>
> When this option is set, synchronization starts automatically, which causes the alternative site to be inconsistent until all pairs in the role pair reach a Prepared state.

Accessibility features for IBM Copy Services Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Copy Services Manager:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

Keyboard navigation

Use the following key combinations to navigate the interface by keyboard:

- To go directly to the topic pane, press Alt+K, and then press Tab.
- In the topic pane, to go to the next link, press Tab.
- To go directly to the Search Results view, press Alt+R, and then press the Enter or Up-Arrow key to enter the view.
- To go directly to the Navigation (Table of Contents) view, press Alt+C, and then press the Enter or Up-Arrow key to enter the view.
- To expand and collapse a node in the navigation tree, press the Right and Left-Arrow keys.
- To move to the next topic node, press the Down-Arrow or Tab key.
- To move to the previous topic node, press the Up-Arrow key or Shift+Tab.
- To go to the next link, button, or topic node from inside on of the views, press Tab.
- To scroll all the way up or down in a pane, press Home or End.
- To go back, press Alt+Left Arrow; to go forward, press Alt+Right Arrow.
- To go to the next pane, press F6.
- To move to the previous pane, press Shift+F6.
- To print the active pane, press Ctrl+P.

IBM and accessibility

For more information about IBM's commitment to accessibility, see the IBM Human Ability and Accessibility Center website at ↪ http://www.ibm.com/able.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBMproducts. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative
work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _enter the year or years_.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at www.ibm.com/privacy/us/en and IBM's Online Privacy Statement at

www.ibm.com/privacy/details/us/en in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Index

U

uninstalling 37
uninstalling Copy Services Manager on distributed systems 23
updating license files 26
upgrading
   disaster recovery capable 43
   from a previous version of Copy Services Manager 43
   upgrading
      from Tivoli Storage Productivity Center for Replication to Copy Services Manager 43

V

verifying 36

W

websites viii

Z

z/OS 5, 30
zFS, migrating to 17

IBM®