IBM

z Systems

Secure Service Container User's Guide

SC28-6971-01

z Systems

Secure Service Container User's Guide

SC28-6971-01

Note

Before you use this information and the product it supports, read the information in “Safety” on page vii, “Notices,” on page 57 and *IBM Systems Environmental Notices and User Guide*, Z125–5823.

This edition, SC28-6971-01, applies to IBM z Systems (z Systems) and IBM LinuxONE (LinuxONE) servers. This edition replaces SC28-6971-00.

There might be a newer version of this document in a **PDF** file available on **Resource Link**. Go to http://www.ibm.com/servers/resourcelink and click **Library** on the navigation bar. A newer version is indicated by a lowercase, alphabetic letter following the form number suffix (for example: 00a, 00b, 01a, 01b).

© Copyright IBM Corporation 2016, 2017.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures v

Safety vii

Safety notices vii

World trade safety information. vii

Laser safety information vii

Laser compliance vii

About this publication ix

Intended audience ix

Prerequisite and related information ix

Related HMC and SE console information . . . x

How to use this publication x

Accessibility x

Accessibility features x

Keyboard navigation x

IBM and accessibility x

How to send your comments xi

Summary of changes xiii

Part 1. Introduction to the IBM Secure Service Container 1

Chapter 1. Secure Service Container: A container technology for deploying appliances 3

Chapter 2. Prerequisites for using Secure Service Container 7

Part 2. Working with Secure Service Container partitions on a standard mode system 11

Chapter 3. Configuring a Secure Service Container partition on a standard mode system. 13

Chapter 4. Starting a Secure Service Container partition on a standard mode system. 19

Chapter 5. Changing the logon settings for a Secure Service Container partition on a standard mode system . 21

Chapter 6. Changing the network settings for a Secure Service Container partition on a standard mode system . 23

Chapter 7. Deactivating or deleting a Secure Service Container partition on a standard mode system. 25

| **Part 3. Working with Secure Service Container partitions on a DPM-enabled system 27**

| **Chapter 8. Creating a Secure Service Container partition on a DPM-enabled system. 29**

| **Chapter 9. Starting a Secure Service Container partition on a DPM-enabled system. 35**

| **Chapter 10. Changing the login settings for a Secure Service Container partition on a DPM-enabled system . . 37**

| **Chapter 11. Changing the network settings for a Secure Service Container partition on a DPM-enabled system . . 39**

| **Chapter 12. Stopping or deleting a Secure Service Container partition on a DPM-enabled system 41**

Part 4. Software appliances 43

Chapter 13. Installing a new software appliance in a Secure Service Container partition 45

Chapter 14. Using the Secure Service Container user interface 49

Requesting and downloading dumps 50

Exporting or importing appliance configuration data 51

Chapter 15. Moving an existing software appliance into a different Secure Service Container partition. . . 53

Part 5. Appendixes. 55

© Copyright IBM Corp. 2016, 2017

Appendix. Notices 57
Trademarks 58
Class A Notices 58

Index 63

Figures

1. A portion of the General page of the Customize/Delete Activation Profiles task. . . 4
2. A portion of the Name page of the New Partition task in basic mode 4
3. A Secure Service Container partition that shows Secure Service Container components 5
4. LPAR image profile: SSC page elements 15
5. A portion of the Name page of the New Partition task in basic mode 30
6. Portion of a Start task window with the successful completion indicated in the Details column 35
7. Sample display of Operating System Messages 45

© Copyright IBM Corp. 2016, 2017

Safety

Safety notices

Safety notices may be printed throughout this guide. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs.

World trade safety information

Several countries require the safety information contained in product publications to be presented in their translation. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the translated safety information with references to the US English source. Before using a US English publication to install, operate, or service this IBM® product, you must first become familiar with the related safety information in the *Systems Safety Notices*, G229-9054. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Laser safety information

All IBM z Systems® (z Systems®) and IBM LinuxONE™ (LinuxONE) models can use I/O cards such as FICON®, Open Systems Adapter (OSA), InterSystem Channel-3 (ISC-3), or other I/O features which are fiber optic based and utilize lasers (short wavelength or long wavelength lasers).

Laser compliance

All lasers are certified in the US to conform to the requirements of DHHS 21 CFR Subchapter J for Class 1 or Class 1M laser products. Outside the US, they are certified to be in compliance with IEC 60825 as a Class 1 or Class 1M laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION: Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION: This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

© Copyright IBM Corp. 2016, 2017

About this publication

This book describes how to use the IBM Secure Service Container to install and run software appliances on IBM z Systems™ (z Systems) and IBM LinuxONE (LinuxONE) servers. Topics include how to configure and start a Secure Service Container partition, and how to install a software appliance using the Secure Service Container installer.

Figures included in this document illustrate concepts and are not necessarily accurate in content, appearance, or specific behavior.

Intended audience

The primary audience for this book is system administrators who are responsible for developing, installing, and managing software that runs in a partition on a z Systems or LinuxONE server.

Prerequisite and related information

For its initial release, the IBM Secure Service Container was known as the z Appliance Container Infrastructure (zACI), which is documented in *IBM z Systems Appliance Container Infrastructure (zACI) User's Guide*, SC28-6970.

This book, SC28-6971, documents the Secure Service Container that is available with Hardware Management Console (HMC) / Support Element (SE) Version 2.13.1, starting with the following engineering change (EC) microcode levels (MCLs):

- SE-BCINST P08458.029
- HMC-SYSTEM P08462.248
- SE-SYSTEM P00339.289

For information about the HMC/SE, see the following resources.

- Information about HMC/SE tasks is available in the console help or IBM Knowledge Center, as described in "Related HMC and SE console information" on page x.
- HMC/SE tasks can be accomplished programmatically as well, through the HMC Web Services application programming interfaces (APIs). For information about APIs, see *z Systems Hardware Management Console Web Services API*, SC27-2634, which is available through the Publications link on IBM Resource Link® at http://www.ibm.com/servers/resourcelink

You can configure Secure Service Container partitions on the following z Systems and LinuxONE servers:

- An IBM z13™ (z13™) or IBM z13s™ (z13s™)
- An IBM LinuxONE Emperor™ (Emperor) or IBM LinuxONE Rockhopper™ (Rockhopper)

For more information about specific mainframes, see the appropriate product document on the IBM Redbooks® website at http://www.redbooks.ibm.com/

- *IBM z13 Technical Guide*, SG24-8251
- *IBM z13s Technical Guide*, SG24-8294

For more information about configuring partitions on a z Systems or LinuxONE server, see the following resources.

- *z Systems PR/SM Planning Guide*, SB10-7162
- *IBM Dynamic Partition Manager Guide*, SB10-7168

© Copyright IBM Corp. 2016, 2017

If your company has the IBM zAware hardware feature on a supported z Systems or LinuxONE server, you can install IBM zAware in a Secure Service Container partition. For additional details and instructions, see *z Advanced Workload Analysis Reporter (IBM zAware) Guide*, SC27-2632.

Related HMC and SE console information

Hardware Management Console (HMC) and Support Element (SE) information can be found on the console help system, or on the IBM Knowledge Center at http://www.ibm.com/support/knowledgecenter/. Click **Select a product**, and then select your server.

How to use this publication

This book provides an overview of the IBM Secure Service Container, and lists the system requirements for its use. This book also provides step-by-step instructions for system administrators who create Secure Service Container partitions, and install software in them. For a list of topics, see "Contents" on page iii.

Accessibility

IBM strives to provide products with usable access for everyone, regardless of age or ability.

Accessible publications for this product are offered in HTML format and can be downloaded from Resource Link at http://www.ibm.com/servers/resourcelink.

If you experience any difficulty with the accessibility of any IBM z Systems® (z Systems®) and IBM LinuxONE (LinuxONE) information, go to Resource Link at http://www.ibm.com/servers/resourcelink and click **Feedback** from the navigation bar on the left. In the **Comments** input area, state your question or comment, the publication title and number, choose **General comment** as the category and click **Submit**. You can also send an email to reslink@us.ibm.com providing the same information.

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

Accessibility features

The following list includes the major accessibility features in z Systems® and IBM LinuxONE documentation:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Customizable display attributes such as color, contrast, and font size
- Communication of information independent of color
- Interfaces commonly used by screen magnifiers
- Interfaces that are free of flashing lights that could induce seizures due to photo-sensitivity.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

IBM and accessibility

See http://www.ibm.com/able for more information about the commitment that IBM has to accessibility.

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. Send your comments by using Resource Link at http://www.ibm.com/servers/resourcelink. Click **Feedback** on the navigation bar on the left. You can also send an email to reslink@us.ibm.com. Be sure to include the name of the book, the form number of the book, the version of the book, if applicable, and the specific location of the text you are commenting on (for example, a page number, table number, or a heading).

Summary of changes

For the most recent edition only, technical changes to the text are indicated by a vertical bar (|) to the left of the change.

Summary of changes for SC28-6971-01

This edition contains the following updates. If a specific update is available through an engineering change (EC) microcode control level (MCL) for the host system, the MCL number is provided.

New information

The topics in Part 3, "Working with Secure Service Container partitions on a DPM-enabled system," on page 27 describe how to create, start, and manage a Secure Service Container partition on a host system with IBM Dynamic Partition Manager (DPM) enabled. DPM supports Secure Service Container partitions starting with EC MCLs HMC-SYSTEM P08462.261 and SE-SYSTEM P00339.304.

Changed information

- The topic, Chapter 2, "Prerequisites for using Secure Service Container," on page 7, contains several updates:
  - Fibre Channel Protocol (FCP) disks are listed as supported storage devices. The support for FCP disks is available starting with EC MCL SE-FWPART P08442.025.
  - IBM Dynamic Partition Manager (DPM) is listed as a supported host-system environment.
  - IBM Blockchain High Security Business Network is listed as a supported appliance.
- The following chapters contain updates for selecting a FICON or FCP device when installing an appliance:
  - Chapter 13, "Installing a new software appliance in a Secure Service Container partition," on page 45
  - Chapter 15, "Moving an existing software appliance into a different Secure Service Container partition," on page 53
- Various topics throughout this book have been updated with information related to Secure Service Container partitions on a DPM-enabled host system.

© Copyright IBM Corp. 2016, 2017

Part 1. Introduction to the IBM Secure Service Container

This part contains general information about IBM Secure Service Container and the advantages of installing software appliances in a Secure Service Container partition, and the prerequisites for use.

- Chapter 1, “Secure Service Container: A container technology for deploying appliances,” on page 3
- Chapter 2, “Prerequisites for using Secure Service Container,” on page 7

© Copyright IBM Corp. 2016, 2017

Chapter 1. Secure Service Container: A container technology for deploying appliances

The IBM Secure Service Container is a container technology through which you can more quickly and securely deploy firmware and software appliances on IBM z Systems (z Systems) and IBM LinuxONE (LinuxONE) servers.

A Secure Service Container partition is a specialized container for installing and running specific firmware or software appliances. An *appliance* is an integration of operating system, middleware, and software components that work autonomously and provide core services and infrastructures that focus on consumability and security. *Firmware appliances* are delivered with the mainframe system; *software appliances* are delivered through software distribution channels.

Partition basics

On other platforms, a partition is a portion of the system hard drive that you create to run different operating systems on the same disk, or to give the appearance of separate hard drives for multiple users or other purposes. On a mainframe system, a *logical partition* is a virtual representation of all of the physical hardware resources of that system, which include processors, memory, and input/output (I/O) adapters.

z Systems and LinuxONE servers support several types of partitions. When system administrators define a partition, they specify characteristics that include processor resources, memory resources, and security controls. System administrators use the Hardware Management Console (HMC) to define partition characteristics.

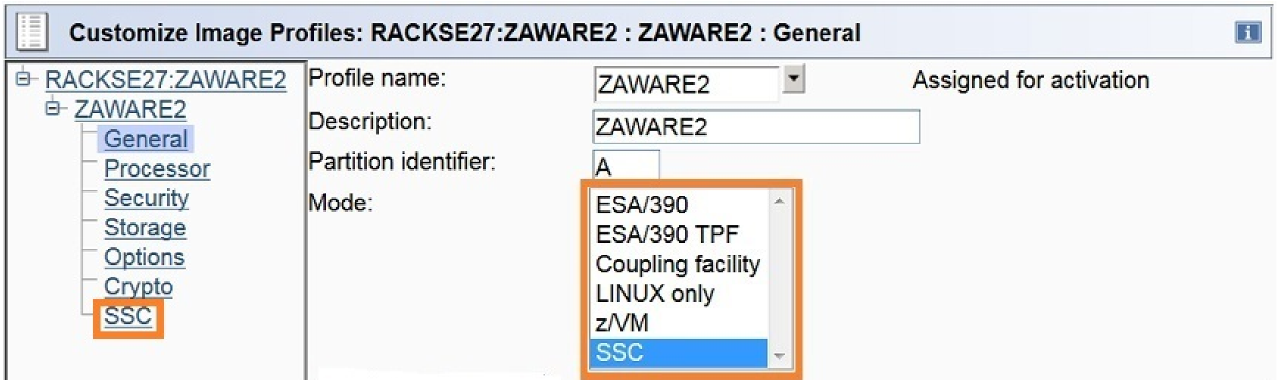
A key partition characteristic is the operating mode, which reflects the specialized function that the partition is to provide, or reflects the operating system or hypervisor that the system administrator wants to load and run in the partition. For example, only the z/VM® operating system can run in a z/VM-mode partition. For such partitions, administrators specify load parameters that define how to install and initialize the operating system.

The host system mode determines which HMC task an administrator uses to define partition characteristics:

- For a host system running in standard mode (that is, with Processor Resource/System Manager or PR/SM™), administrators use the **Customize/Delete Activation Profiles** task to define the operating mode of a partition. For a Secure Service Container partition, the operating mode is **SSC**.

  Figure 1 on page 4 shows a sample screen capture of the **Customize/Delete Activation Profiles** task page through which an administrator selects the partition mode. To configure a Secure Service Container partition, an administrator selects **SSC** as the Mode value.

© Copyright IBM Corp. 2016, 2017



Customize Image Profiles: RACKSE27:ZAWARE2 : ZAWARE2 : General

Profile name: ZAWARE2 Assigned for activation

Description: ZAWARE2

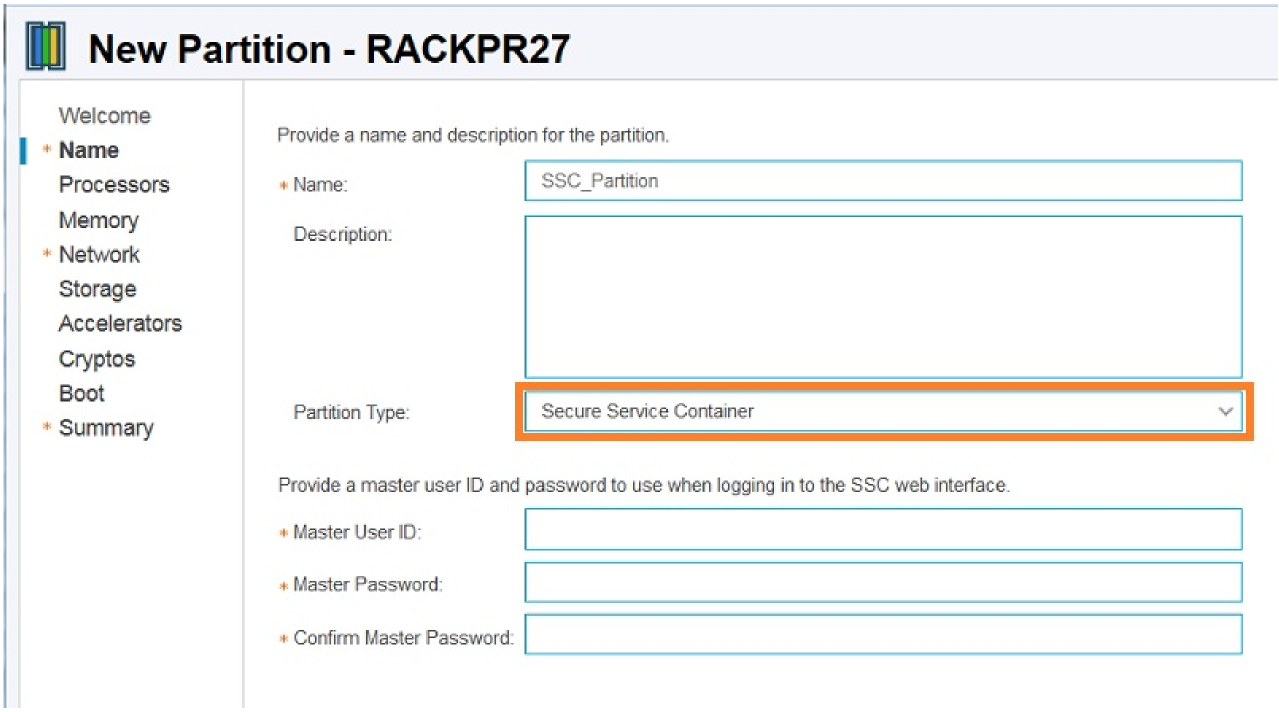
Partition identifier: A

Mode: ESA/390, ESA/390 TPF, Coupling facility, LINUX only, z/VM, SSC (selected)

Figure 1. A portion of the General page of the Customize/Delete Activation Profiles task

- For a host system with IBM Dynamic Partition Manager (DPM) enabled, administrators use the **New Partition** task to select the partition type. For a Secure Service Container partition, the partition type is **Secure Service Container**.

  Figure 2 shows a sample screen capture of the **New Partition** task (in basic mode) through which an administrator selects the partition type. To configure a Secure Service Container partition, an administrator selects **Secure Service Container** as the type value.



New Partition - RACKPR27

Provide a name and description for the partition.

* Name: SSC_Partition

Description:

Partition Type: Secure Service Container

Provide a master user ID and password to use when logging in to the SSC web interface.

* Master User ID:

* Master Password:

* Confirm Master Password:

Figure 2. A portion of the Name page of the New Partition task in basic mode

What makes a Secure Service Container partition different from other partitions

Unlike most other types of partitions, a Secure Service Container partition contains its own embedded operating system, security mechanisms, and other features that are specifically designed for simplifying the installation of appliances, and for securely hosting them. Figure 3 provides a high-level view of the Secure Service Container components for hosting appliances.

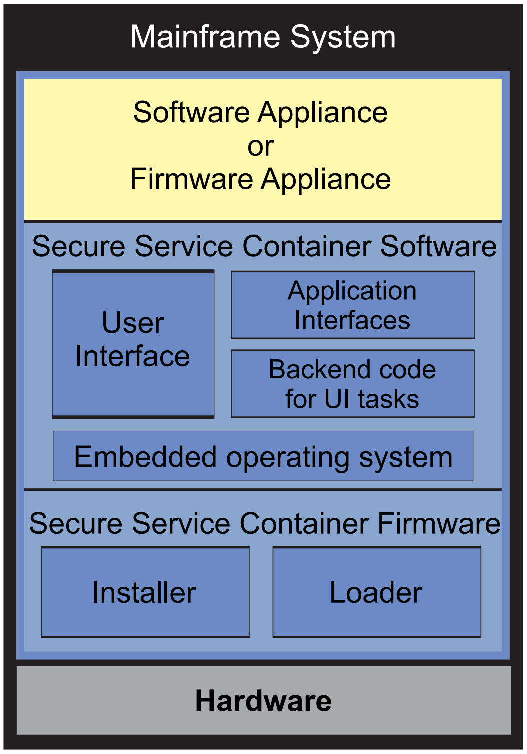

Mainframe System
Software Appliance or Firmware Appliance
Secure Service Container Software
User Interface
Application Interfaces
Backend code for UI tasks
Embedded operating system
Secure Service Container Firmware
Installer
Loader
Hardware

Figure 3. A Secure Service Container partition that shows Secure Service Container components

Through these components, Secure Service Container provides:

- Quicker and simpler installation of firmware and software appliances
- End-to-end appliance tamper protection
- Protected intellectual property of appliance components

For a list of supported appliances and the requirements for their installation in a Secure Service Container partition, see Chapter 2, “Prerequisites for using Secure Service Container,” on page 7.

Chapter 2. Prerequisites for using Secure Service Container

This topic provides information about the IBM z Systems (z Systems) and IBM LinuxONE (LinuxONE) servers that contain the IBM Secure Service Container.

You can configure Secure Service Container partitions on the following z Systems and LinuxONE servers.

- An IBM z13 (z13) or IBM z13s™ (z13s™)
- An IBM LinuxONE Emperor (Emperor) or IBM LinuxONE Rockhopper (Rockhopper)

To configure a Secure Service Container partition, you need to use Hardware Management Console (HMC) / Support Element (SE) Version 2.13.1 or later. The suggested practice is to use the latest available firmware for Secure Service Container, which is identified by the engineering change (EC) SE-BCINST P08458. To find the latest available EC microcode control levels (MCLs) for Secure Service Container, use the instructions for hardware updates in "Where to find hardware planning and corequisite software information" on page 9.

Before you configure a Secure Service Container partition

The host system mode determines which HMC task you can use to define a Secure Service Container partition.

- For a host system running in standard mode (that is, with Processor Resource/System Manager or PR/SM), use the **Customize/Delete Activation Profiles** task.
- For a host system with IBM Dynamic Partition Manager (DPM) enabled, use the **New Partition** task. To create a Secure Service Container partition on a DPM-enabled system, you must install EC MCLs HMC-SYSTEM P08462.261 and SE-SYSTEM P00339.304 or later.

Before you use either task to create a partition, make sure that your installation meets the following prerequisites.

- Your installation must have correctly configured the z Systems or LinuxONE server (or central processor complex or CPC) on which you want to configure the Secure Service Container partition.
- Before you create a Secure Service Container partition, use the appropriate method to specify the activation order for the new partition.
  - For a host system running in standard mode, update the CPC reset profile to include the activation order for the new partition.
  - For a host system with DPM enabled, update the Start Options section of the **System Details** task.
- Before starting the Secure Service Container partition, make sure that I/O and storage devices have been configured for this partition. The I/O and storage device requirements depend on the appliance that you plan to install.
  - Supported network options are HiperSockets™ or any Open Systems Adapter (OSA) features that are configured on the system. For OSA features:
    - Secure Service Container can use only port 0. Other types of partitions can use port 1 of the same OSA feature.
    - If you have multiple Secure Service Container partitions running on the same system, they can share the same OSA feature. From a security point of view, however, a dedicated I/O resource is more secure than a shared one. So if the appliance that you install in a Secure Service Container partition requires a high level of security, consider configuring the OSA feature as dedicated rather than shared.

© Copyright IBM Corp. 2016, 2017

- Supported storage devices are Extended Count Key Data (ECKD™) and Fibre Channel Protocol (FCP) disks. The support for FCP disks is available starting with EC MCL SE-FWPART P08442.025. Target FCP disks must be large enough to fit the uncompressed appliance, with an additional 2 GB for the Secure Service Container installer to use.

  To enable Secure Service Container to discover FCP disks on which you can install software appliances, your installation needs to verify that the logical unit numbers (LUNs) for these disks are mapped to the appropriate host/initiator world wide port names (WWPNs), and to enable N Port Identifier Virtualization (NPIV) through the Support Element. To enable NPIV, complete the following steps.

  1. On the HMC, log on to the Support Element through the **Single Object Operations** task, with a user ID that is associated with the operator, advanced operator, system programmer, or service representative role.
  2. Locate the channel path identifier (CHPID) that provides access to the FCP devices.
  3. Locate and open the **FCP NPIV Mode On/Off** task.
  4. On the NPIV Mode On/Off window, select the listed channel paths to be enabled for FCP NPIV mode, and click **Apply**.

The host system mode determines how to define network connections and storage devices for this partition.

- For a host system running in standard mode, you use either the Hardware Configuration Definition (HCD) or the Input/Output Configuration Program (IOCP). Depending on the tool you are using, you might need to use the instructions in one of the following books:
  - *z/OS® Hardware Configuration Definition User's Guide*, SC33-7988, and *z/OS Hardware Configuration Definition Scenarios*, SC33-7987
  - *z Systems Input/Output Configuration Program User's Guide for ICP IOCP*, SB10-7163

  - For a host system with DPM enabled, use the Hardware Management Console (HMC) **Manage Adapters** task. For more information, see *IBM Dynamic Partition Manager Guide*, SB10-7168. To create a Secure Service Container partition on a DPM-enabled system, you must install EC MCLs HMC-SYSTEM P08462.261 and SE-SYSTEM P00339.304.

    Note: For appliances that run in a Secure Service Container partition on a DPM-enabled system, you can configure only Fibre Channel Protocol (FCP) disks for storage.

Firmware and software appliances that can be installed in a Secure Service Container partition

Secure Service Container supports the following firmware and software appliances.

- IBM Blockchain High Security Business Network. For more information, see the IBM announcement at https://www.ibm.com/common/ssi/cgi-bin/ssialias?infotype=an&subtype=ca&appname=gpateam&supplier=897&letternum=ENUS216-491
- IBM z/VSE® Network Appliance (VNA). This software appliance is available for download through the z/VSE website: http://www.ibm.com/systems/z/os/zvse/
- The IBM z Advanced Workload Analysis Reporter (IBM zAware) Software Appliance. For more information, go to the web page for IBM Operations Analytics for z Systems Version 3.1 at http://www.ibm.com/software/products/en/ibm-operations-analytics-for-z-systems
- The IBM z Advanced Workload Analysis Reporter (IBM zAware) firmware appliance, which requires hardware feature code 0011 on the z Systems or LinuxONE server. This firmware appliance is available with the server when customers order the server with feature code 0011.

The following requirements apply for all supported appliances:

- Only one appliance can be installed and run in a Secure Service Container partition at any given time; this type of partition does not support running multiple appliances simultaneously.
- You can define more than one Secure Service Container partition on the same system, and run instances of the same appliance in each one. In this case, each partition must use separate storage devices.
- You can reuse an existing Secure Service Container partition for a different appliance. After stopping the installed appliance and the partition, reboot the Secure Service Container installer and select a different appliance to install. Before doing so, however, check the storage and network connections for the partition to make sure that they are appropriate for the appliance to be installed.

Where to find hardware planning and corequisite software information

For the most recent hardware planning and corequisite software information, go to IBM Resource Link:

`http://www.ibm.com/servers/resourcelink`

- For hardware updates, click **Tools** on the navigation panel. Then click **Machine information** under **Servers**, and enter your enterprise number, customer number, or machine serial number for the host system (CPC). You must register with IBM to search machine information.
- For software updates, click **Fixes** on the navigation panel. Then click **Preventative Service Planning buckets (PSP)** under **Preventive actions**, and check the PSP bucket for the appropriate server.:
  - For a z13 or Emperor, the 2964DEVICE PSP bucket
  - For a z13s™ or Rockhopper, the 2965DEVICE PSP bucket

Part 2. Working with Secure Service Container partitions on a standard mode system

This part contains step-by-step instructions for initially configuring and starting a Secure Service Container partition on a host system that is running in standard mode (that is, with Processor Resource/System Manager or PR/SM). Topics include instructions for resetting login and network values.

- Chapter 3, "Configuring a Secure Service Container partition on a standard mode system," on page 13
- Chapter 4, "Starting a Secure Service Container partition on a standard mode system," on page 19
- Chapter 5, "Changing the logon settings for a Secure Service Container partition on a standard mode system," on page 21
- Chapter 6, "Changing the network settings for a Secure Service Container partition on a standard mode system," on page 23

© Copyright IBM Corp. 2016, 2017

Chapter 3. Configuring a Secure Service Container partition on a standard mode system

Use this procedure to configure a Secure Service Container partition on a host system that is running in standard mode (that is, with Processor Resource/System Manager or PR/SM). These configuration instructions include setting initial logon and network values. This procedure is intended for experienced system administrators or system programmers who are responsible for configuring logical partitions on z Systems and LinuxONE servers. To configure a Secure Service Container partition on a standard mode system, use the Hardware Management Console (HMC) **Customize/Delete Activation Profiles** task to create an image profile. Depending on the IT roles and responsibilities at your installation, you might need to collaborate with network administrators to complete specific configuration tasks.

Before you begin

- Check the list of prerequisites and information sources in Chapter 2, "Prerequisites for using Secure Service Container," on page 7.
- Make sure that the image profile name that you supply for the Secure Service Container partition is the same as the name of an LPAR image in the input/output configuration data set (IOCDS) for the CPC. Otherwise, the partition cannot be activated.
- To prepare to use the HMC to configure the Secure Service Container partition, make sure that you log in to the HMC with a user ID that is assigned to the system programmer role (SYSPROG).

About this task

This procedure includes only the instructions that are required to use the HMC **Customize/Delete Activation Profiles** task to supply specific LPAR characteristics for a Secure Service Container partition. If you need additional information about other LPAR characteristics that you can specify through this task, see the HMC online help.

If your company has the IBM zAware hardware feature on a supported z Systems or LinuxONE server, you can install the IBM zAware firmware appliance in a Secure Service Container partition. In this case, use the instructions for configuring a Secure Service Container partition in *z Advanced Workload Analysis Reporter (IBM zAware) Guide*, SC27-2632.

Procedure

1. Through the HMC, select the CPC and open the **Customize/Delete Activation Profiles** task. Select the LPAR that you want to either create or customize as a Secure Service Container partition. The remaining steps in this procedure illustrate how to customize an existing image profile; however, you can use this information to help you create an image profile through the **New Image Profile** wizard.
2. On the Customize Image Profiles window, select the **General** page from the profile tree view to define the partition mode and other characteristics.
   a. If you are using the default image profile or an existing image profile as a template for a new image profile, or you selected the default image profile, supply a new name for this image profile by typing over the displayed name before you make any other changes, and click **Save** to save the profile with the new name.

      A profile name can be 1 - 8 characters long. It cannot have special characters or imbedded blanks. Valid characters for a profile name are:

      Characters 0 - 9
      Decimal digits

      Characters A - Z
      Letters of the English alphabet

© Copyright IBM Corp. 2016, 2017

Profile names are not case-sensitive. All alphabetic characters are saved in uppercase.

b. For **Mode**, select **SSC** mode from the scrollable list. When you select **SSC** as the partition mode, the HMC adjusts the navigation pane and individual page content to display LPAR characteristics that are appropriate for a Secure Service Container partition. The profile tree view now contains a link for the **SSC** page.

c. Provide or modify any remaining values on the **General** page, using the online help for guidance.

3. Select the **Processor** page and specify the processor requirements for the appliance that you plan to install in the Secure Service Container partition. If necessary, use the online help for guidance.

   Secure Service Container does not require any processing resources, so specify the values that are required for only the appliance to be installed. You can assign only one of two processor types for the Secure Service Container partition: Integrated facilities for Linux (IFLs) or central processors (CPs). The IFLs or CPs can be shared or dedicated. The available processor types vary by host system; for example, both IFLs and CPs are available on a z13, but only IFLs are available on an Emperor.

4. Select the **Security** page and provide or modify any values as appropriate for the appliance that you plan to install. If necessary, use the online help for guidance.

   You can specify any partition security options for this partition. Select the remaining options according to the requirements of the appliance.

5. Select the **Storage** page and specify the amount of central and expanded storage that is required for the appliance that you plan to install. If necessary, use the online help for guidance.

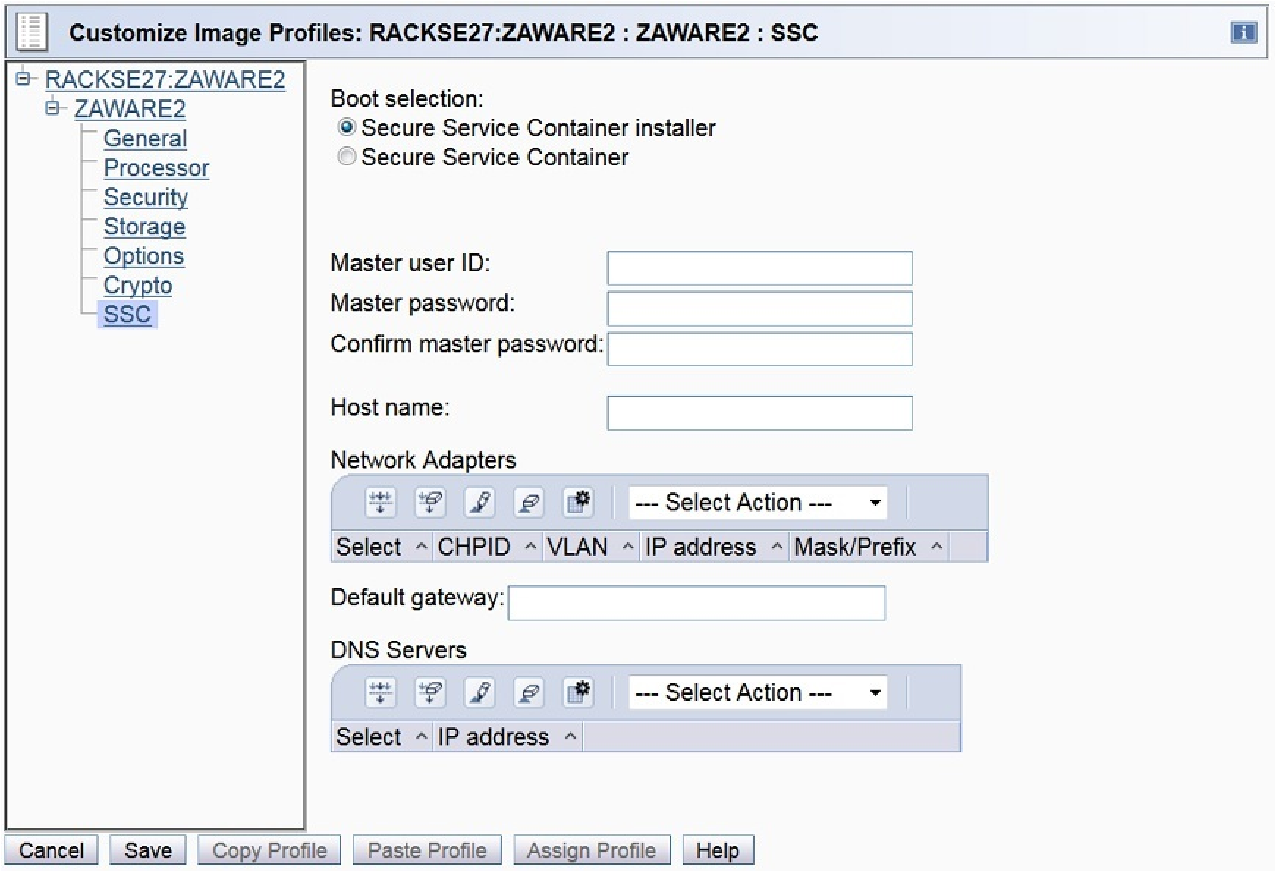
   Although the storage amounts that you specify are based on the requirements of the appliance that you plan to install, note that a minimum of 4096 MB (4 GB) of central storage is required to activate the Secure Service Container partition.

6. Select the **Options** page and provide or modify any values as appropriate for the appliance that you plan to install. If necessary, use the online help for guidance.

7. Select the **Cryptos** page and provide or modify any cryptographic controls as appropriate for the appliance that you plan to install. If necessary, use the online help for guidance.

8. Select the **SSC** page in the profile tree view.

   Figure 4 on page 15 shows the **SSC** page elements.



Customize Image Profiles: RACKSE27:ZAWARE2 : ZAWARE2 : SSC

Boot selection:
● Secure Service Container installer
○ Secure Service Container

Master user ID:
Master password:
Confirm master password:

Host name:

Network Adapters

Select	CHPID	VLAN	IP address	Mask/Prefix

Default gateway:

DNS Servers

Select	IP address

Figure 4. LPAR image profile: SSC page elements

a. Under Boot selection, note that only one option is selectable: **Secure Service Container installer**

b. Provide values for the default master user ID and password.

Master user ID

Enter the user ID to be used as the default master user ID for the Secure Service Container partition. This user ID has authority to perform any task that is available through the Secure Service Container graphical user interface (GUI).

A master user ID can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: period (.), underscore (_), and hyphen (-).

Master password

Enter the password for the master user ID. A master password can have a minimum of 8 characters and a maximum of 256 characters. A master password is case-sensitive and can contain numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: hyphen (-), underscore (_), exclamation (!), at (@), hash (#), dollar ($), percent (%), carat (^), ampersand (&), asterisk (*), left parenthesis ((), right parenthesis ()), plus (+), left brace ({), right brace (}), vertical bar (|), colon (:), less than (<), greater than (>), question mark (?), and equals (=).

Confirm master password

Reenter the password exactly as you typed it for the Master password field.

c. Provide a value for the host name.

A host name can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: period (.), colon (:), and hyphen (-).

d. Customize the network adapter configuration for the Secure Service Container partition.

1) From the **Select Action** list in the Network Adapters table, click **Add/Edit Network Adapters** to define a network connection. The Add/Edit Network Adapters Entry window is displayed.

2) For each type of network connection in the Secure Service Container environment, supply the following information.

For example, if the appliance to be installed uses a HiperSockets subnet for communication, and Secure Service Container administrators are using an Open Systems Adapter (OSA) channel to access the Secure Service Container GUI, you need to define two network adapters: one for the HiperSockets subnet and another for the OSA channel.

IP address type
Select one of the following types:
- Dynamic Host Connection Protocol (DHCP)
- Link local addressing
- Static IPv4 Address
- Static IPv6 Address (This option is supported only for the IBM zAware firmware appliance.)

The type you select determines which of the remaining fields you can complete; if a field does not apply for a specific selected type, you cannot enter a value.

CHPID
Enter the logical channel path identifier (CHPID) of the network adapter. You can specify the same CHPID multiple times.

Note:
- For an Open Systems Adapter (OSA) card, you can use only port 0.
- Because of unpredictable behavior in the address resolution protocol, the suggested practice is to use only one CHPID for IP addresses on the same subnet. If you use more than one CHPID with IP addresses on the same subnet, a significant amount of time might be required before all IP addresses are reachable (it could take up to a day for larger network environments).

VLAN Specify the virtual local area network (VLAN) if the link you are using is defined in `TRUNK` mode. The valid range of VLAN IDs is 1 - 4094.

IP Address
Enter the IP address of the network adapter. This field is available only for IP addresses of type **Static IPv4 Address** and **Static IPv6 Address**.

Mask/Prefix
For an IPv4 or IPv6 address, optionally specify the 2-digit mask/prefix. If you need to convert a 4-byte subnet mask to the 2-digit format, you can find several subnet mask converters on the Internet.

For network connections:
- You can define 1 - 100 connections.
- You can define multiple connections using the same CHPID.
- You can assign IP addresses of both types **Static IPv4 Address** and **Static IPv6 Address** to the same CHPID/VLAN set. To do so requires one connection entry for IPv4 and another connection entry for IPv6.

3) Click **OK** to save your changes and return to the previous page.

e. Customize global network attributes for the Secure Service Container partition.

1) In the **Default gateway** field, enter an IPv4 address for the default gateway.

Note: Only IPv4 is supported.

    2) From the **Select Action** list in the DNS Servers table, click **Add/Edit DNS server** to define a primary domain name system (DNS) server. The Add/Edit DNS Entry window is displayed. You can define a maximum of two DNS entries.

       A DNS server definition is required if you specified a DHCP-type IP address for any of the network adapters for the Secure Service Container partition.

    3) Enter the IPv4 or IPv6 address of the DNS server.
    4) Click **OK** to save your changes and return to the **SSC** page.

9. Click **Save** when you finish working with the image profile for the Secure Service Container partition. The HMC displays a message indicating the status of the save operation.

Results

The image profile for the Secure Service Container partition is complete.

What to do next

Activate the Secure Service Container partition by following the instructions in Chapter 4, "Starting a Secure Service Container partition on a standard mode system," on page 19.

If you need to modify the logon or network settings at a later time, see the instructions in the following topics:

- Chapter 5, "Changing the logon settings for a Secure Service Container partition on a standard mode system," on page 21
- Chapter 6, "Changing the network settings for a Secure Service Container partition on a standard mode system," on page 23

Chapter 4. Starting a Secure Service Container partition on a standard mode system

Use this procedure to start a Secure Service Container partition through the Hardware Management Console (HMC) on a host system that is running in standard mode (that is, with Processor Resource/System Manager or PR/SM).

Before you begin

- Before activating the Secure Service Container partition, make sure that I/O and storage devices have been configured for this partition in the I/O definition file (IODF) or I/O configuration data set (IOCDS) that is currently in effect for the host system. The I/O and storage device requirements depend on the appliance that you plan to install.
- To activate the Secure Service Container partition, make sure that you log in to the HMC with a user ID that is assigned to one of the following roles: SYSPROG, OPERATOR, or ADVANCED.

Procedure

1. Select the image for the Secure Service Container partition.
2. From the **Daily** task group, open the **Activate** task. The Activate Task Confirmation window is displayed.
3. Review the confirmation text to decide whether to proceed with the task. If you want to continue this task, click **Yes**. The Activate Progress window opens to indicate the progress of the activation and the outcome.
4. Click **OK** to close the window when the activation completes successfully.

   Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Results

When the Secure Service Container partition is activated, the sequence of events varies, depending on which boot selection you specified on the **SSC** page of the image profile.

Secure Service Container Installer

With this boot selection, the partition start process initializes the Secure Service Container Installer so you can install an appliance. This boot selection is the only option when you start a newly configured Secure Service Container partition for the first time. With this option, the Secure Service Container Installer is started automatically. When the start process completes, you can access the Secure Service Container Installer through your choice of browser. For more instructions, see the appropriate installation topic in Part 4, "Software appliances," on page 43.

Secure Service Container

With this boot selection, the partition start process effectively restarts an installed appliance. If you previously used the Secure Service Container Installer to successfully install a firmware or software appliance, this boot selection becomes the default selection in the image profile for the Secure Service Container partition. In this case, the Secure Service Container Installer is rebooted, and the installed appliance is restarted in the Secure Service Container partition on this and all subsequent reboots, until you change the boot selection in the image profile.

What to do next

- If you have activated a new Secure Service Container partition for the first time, connect to the Secure Service Container installer through the browser of your choice, and install a software appliance. For instructions, see the appropriate topic in Part 4, "Software appliances," on page 43.

© Copyright IBM Corp. 2016, 2017

If your company has the IBM zAware hardware feature on a supported z Systems or LinuxONE server, you can install IBM zAware in a Secure Service Container partition. For additional details and instructions, see *z Advanced Workload Analysis Reporter (IBM zAware) Guide*, SC27-2632.

- If a previously installed appliance has been restarted, use the IP address to connect to the appliance. For additional details, see the product documentation for the installed appliance.

Chapter 5. Changing the logon settings for a Secure Service Container partition on a standard mode system

Use this procedure when you need to change the current logon settings for a Secure Service Container partition on a host system that is running in standard mode (that is, with Processor Resource/System Manager or PR/SM). This procedure is intended for experienced system administrators or system programmers who are responsible for configuring logical partitions on z Systems and LinuxONE servers. To modify the logon settings of a Secure Service Container partition, use the Hardware Management Console (HMC) **Customize/Delete Activation Profiles** task to modify the partition profile.

Before you begin

Make sure that you log in to the HMC with a user ID that is assigned to the system programmer role (SYSPROG).

About this task

A system administrator might need to change the current logon settings for the partition, for example, to comply with company rules for changing passwords. An administrator also might change the master ID and password for the partition if the ID and password values are forgotten or lost.

Procedure

1. From the Systems Management menu on the HMC, select the system on which you created the Secure Service Container partition, and select that partition in the Partitions list. From the Operational Customization Tasks group, open the **Customize/Delete Activation Profiles** task.
2. On the Customize Image Profiles window, select the **SSC** page in the profile tree view.
3. On the **SSC** page, click **Reset Logon Settings**. On the resulting confirmation window, click **Yes** to continue.
   a. Replace the current values for the default master user ID and password.

      Master user ID

      Enter the user ID to be used as the default master user ID for the Secure Service Container partition. This user ID has authority to perform any task that is available through the Secure Service Container graphical user interface (GUI).

      A master user ID can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: period (.), underscore (_), and hyphen (-).

      Master password

      Enter the password for the master user ID. A master password can have a minimum of 8 characters and a maximum of 256 characters. A master password is case-sensitive and can contain numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: hyphen (-), underscore (_), exclamation (!), at (@), hash (#), dollar ($), percent (%), carat (^), ampersand (&), asterisk (*), left parenthesis ((), right parenthesis ()), plus (+), left brace ({), right brace (}), vertical bar (|), colon (:), less than (<), greater than (>), question mark (?), and equals (=).

      Confirm master password

      Reenter the password exactly as you typed it for the Master password field.

   b. Replace the current value for the host name.

© Copyright IBM Corp. 2016, 2017

A host name can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: period (.), colon (:), and hyphen (-).

4. Click **Save** when you finish working with the image profile for the Secure Service Container partition. The HMC displays a message indicating the status of the save operation.

Results

The partition profile has been updated with the revised logon settings.

What to do next

Reactivate the Secure Service Container partition by following the instructions in Chapter 4, “Starting a Secure Service Container partition on a standard mode system,” on page 19.

Chapter 6. Changing the network settings for a Secure Service Container partition on a standard mode system

Use this procedure when you need to change the current network settings for a Secure Service Container | partition on a host system that is running in standard mode (that is, with Processor Resource/System | Manager or PR/SM). This procedure is intended for experienced system administrators or system programmers who are responsible for configuring logical partitions on z Systems and LinuxONE servers. To modify the network settings of a Secure Service Container partition, use the Hardware Management Console (HMC) **Customize/Delete Activation Profiles** task to modify the partition profile.

Before you begin

Make sure that you log in to the HMC with a user ID that is assigned to the system programmer role (SYSPROG).

About this task

A system administrator might need to change the current network settings for the partition, for example, when the hardware configuration changes or when an additional network is required.

Procedure

1. From the Systems Management menu on the HMC, select the system on which you created the Secure Service Container partition, and select that partition in the Partitions list. From the Operational Customization Tasks group, open the **Customize/Delete Activation Profiles** task.
2. On the Customize Image Profiles window, select the **SSC** page in the profile tree view.
3. On the **SSC** page, click **Reset Network Settings**. On the resulting confirmation window, click **Yes** to continue.
   a. Modify the network adapter configuration, as necessary.
      1) From the **Select Action** list in the Network Adapters table, click **Add/Edit Network Adapters** to define a network connection. The Add/Edit Network Adapters Entry window is displayed.
      2) For each type of network connection in the Secure Service Container environment, supply the following information.

         IP address type
         Select one of the following types:
         - Dynamic Host Connection Protocol (DHCP)
         - Link local addressing
         - Static IPv4 Address
         - Static IPv6 Address (This option is supported only for the IBM zAware firmware appliance.)

         The type you select determines which of the remaining fields you can complete; if a field does not apply for a specific selected type, you cannot enter a value.

         CHPID
         Enter the logical channel path identifier (CHPID) of the network adapter. You can specify the same CHPID multiple times.

         Note:
         - For an Open Systems Adapter (OSA) card, you can use only port 0.
         - Because of unpredictable behavior in the address resolution protocol, the suggested practice is to use only one CHPID for IP addresses on the same subnet. If you use

© Copyright IBM Corp. 2016, 2017

more than one CHPID with IP addresses on the same subnet, a significant amount of time might be required before all IP addresses are reachable (it could take up to a day for larger network environments).

VLAN Specify the virtual local area network (VLAN) if the link you are using is defined in `TRUNK` mode. The valid range of VLAN IDs is 1 - 4094.

IP Address
Enter the IP address of the network adapter. This field is available only for IP addresses of type **Static IPv4 Address** and **Static IPv6 Address**.

Mask/Prefix
For an IPv4 or IPv6 address, optionally specify the 2-digit mask/prefix. If you need to convert a 4-byte subnet mask to the 2-digit format, you can find several subnet mask converters on the Internet.

For network connections:

- You can define 1 - 100 connections.
- You can define multiple connections using the same CHPID.
- You can assign IP addresses of both types **Static IPv4 Address** and **Static IPv6 Address** to the same CHPID/VLAN set. To do so requires one connection entry for IPv4 and another connection entry for IPv6.

3) Click **OK** to save your changes and return to the previous page.

b. Modify the global network attributes, as necessary.

1) In the **Default gateway** field, enter an IPv4 address for the default gateway.

Note: Only IPv4 is supported.

2) From the **Select Action** list in the DNS Servers table, click **Add/Edit DNS server** to define a primary domain name system (DNS) server. The Add/Edit DNS Entry window is displayed. You can define a maximum of two DNS entries.

A DNS server definition is required if you specified a DHCP-type IP address for any of the network adapters for the Secure Service Container partition.

3) Enter the IPv4 or IPv6 address of the DNS server.

4) Click **OK** to save your changes and return to the **SSC** page.

4. Click **Save** when you finish working with the image profile for the Secure Service Container partition. The HMC displays a message indicating the status of the save operation.

Results

The partition profile has been updated with the revised network settings.

What to do next

Reactivate the Secure Service Container partition by following the instructions in Chapter 4, “Starting a Secure Service Container partition on a standard mode system,” on page 19.

Chapter 7. Deactivating or deleting a Secure Service Container partition on a standard mode system

Use this procedure to deactivate or delete a Secure Service Container partition through the Hardware Management Console (HMC) on a host system that is running in standard (Processor Resource/System Manager or PR/SM) mode. This action is a disruptive task.

Before you begin

To deactivate or delete the Secure Service Container partition, make sure that you log in to the HMC with a user ID that is assigned to one of the following roles: SYSPROG, OPERATOR, or ADVANCED.

About this task

When you determine that you no longer need a Secure Service Container partition, deactivate and then either delete or modify its image profile to avoid inadvertently restarting a firmware or software appliance from a disk that might be in use by another partition.

Procedure

1. To deactivate a Secure Service Container partition, complete the following steps.

   This task stops the installed application and the embedded operating system, and deallocates resources for the selected partition.

   a. Select the image for the Secure Service Container partition.

   b. From the **Daily** task group, open the **Deactivate** task. The Deactivate Task Confirmation window is displayed.

   c. Review the confirmation text to decide whether to proceed with the task. If you want to continue this task, click **Yes**. The Deactivate Progress window opens to indicate the progress of the deactivation and the outcome.

   d. Click **OK** to close the window when the deactivation completes successfully.

      Otherwise, if the deactivation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

2. After the partition is deactivated, you can either delete or modify its image profile to prevent the automatic restart of the partition and its installed application.

   - To delete the image profile:

     a. Select the image for the Secure Service Container partition.

     b. From the Operational Customization Tasks group, open the **Customize/Delete Activation Profiles** task.

     c. Select the image profile for the Secure Service Container partition, and click **Delete**. The HMC displays a message that indicates the status of the delete operation.

   - To modify the image profile:

     a. Select the image for the Secure Service Container partition.

     b. From the Operational Customization Tasks group, open the **Customize/Delete Activation Profiles** task.

     c. Select the image profile for the Secure Service Container partition, and click **Customize profile**.

     d. On the Customize Image Profiles window, select the **SSC** page from the profile tree, and select the **Secure Service Container installer** boot selection.

     e. Click **Save** when you finish working with the image profile for the Secure Service Container partition. The HMC displays a message indicating the status of the save operation.

© Copyright IBM Corp. 2016, 2017

Results

The image profile is either deleted or modified such that an application cannot be restarted in the Secure Service Container partition.

Part 3. Working with Secure Service Container partitions on a DPM-enabled system

This part contains step-by-step instructions for initially configuring and starting a Secure Service Container partition on a host system with IBM Dynamic Partition Manager (DPM) enabled. Topics include instructions for resetting login and network values.

- Chapter 8, “Creating a Secure Service Container partition on a DPM-enabled system,” on page 29
- Chapter 9, “Starting a Secure Service Container partition on a DPM-enabled system,” on page 35
- Chapter 10, “Changing the login settings for a Secure Service Container partition on a DPM-enabled system,” on page 37
- Chapter 11, “Changing the network settings for a Secure Service Container partition on a DPM-enabled system,” on page 39
- Chapter 12, “Stopping or deleting a Secure Service Container partition on a DPM-enabled system,” on page 41

© Copyright IBM Corp. 2016, 2017

Chapter 8. Creating a Secure Service Container partition on a DPM-enabled system

Use this procedure to configure a Secure Service Container partition on a host system with IBM Dynamic Partition Manager (DPM) enabled. These configuration instructions include setting initial logon and network values. This procedure is intended for system administrators or system programmers who are responsible for configuring logical partitions on z Systems and LinuxONE servers. To configure a Secure Service Container partition on a DPM-enabled system, use the Hardware Management Console (HMC) **New Partition** task to create a partition definition.

Before you begin

The **New Partition** task offers two modes through which you can create a partition: basic and advanced. This procedure provides instructions only for the basic mode of the **New Partition** task. However, because the advanced mode is similar, you can use these instructions for the advanced mode as well. Note that some pages, or sections, of the advanced mode might have slightly different names and additional content, compared to the basic mode.

- Check the topic Chapter 2, “Prerequisites for using Secure Service Container,” on page 7 for a list of requirements, including the DPM engineering change (EC) microcode levels (MCLs).
- Make sure you have the appropriate authorization to use the **New Partition** task. You need to use either the default SYSPROG user ID or a user ID that a system administrator has authorized to this task through customization controls in the **User Management** task.
- Use the online help for the **New Partition** task together with these instructions; the online help explains the page elements and functions in more detail. To access the online help, click **Help** on the **New Partition** task window. Note that the basic and advanced modes of the task have separate online help; to access the help for the advanced mode, switch to that mode and then click **Help**.

About this task

The basic mode of the **New Partition** task provides a quick, guided method of creating a partition; DPM either provides default values or automatically generates many of the values for partition properties that are required to successfully start a partition. Some of these properties are not displayed or editable in the basic task mode.

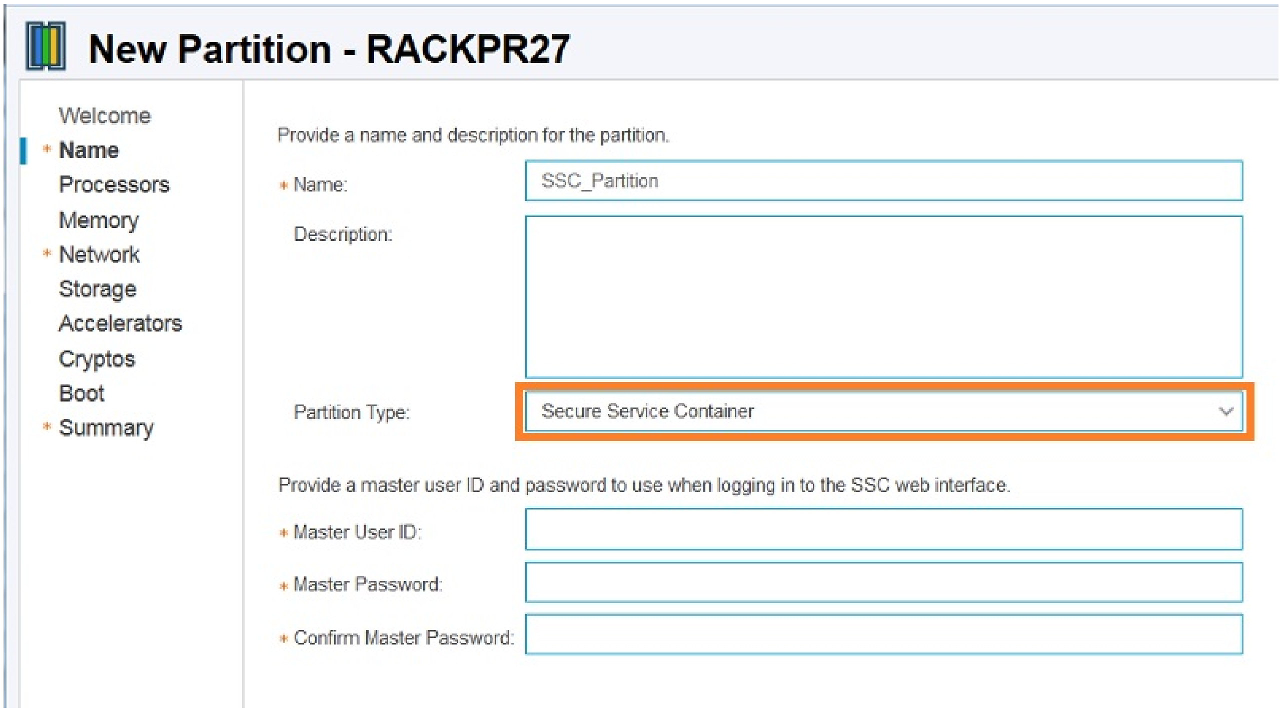
Some of the following individual steps are marked as required, which indicates that the corresponding task page contains fields for which you need to supply a value or make a selection. The end result of the task is a partition definition, which you can modify through the **Partition Details** task, or use to start the partition through the **Start** task.

Procedure

1. Open the **New Partition** task. You can access this task from the main HMC page by selecting the Systems Management node, by selecting a specific DPM-enabled system, or by selecting the task in the Tasks index. For example:
   a. Select a DPM-enabled system listed under the Systems Management node.
   b. From the Configuration task group, click the link for the **New Partition** task. The New Partition window opens, with an overlay that highlights key task controls on the window.
   c. Click the **Okay, got it** button to remove the overlay. The Welcome page is displayed.
   d. Click **Next** to navigate to the next page in the task.

© Copyright IBM Corp. 2016, 2017

2. Required: Use the Name page to enter the name of the new partition, an optional description, and the partition type. A partition name must uniquely identify the partition from all other partitions defined on the same system.
   a. Specify the name of the new partition, which can be 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters.
   b. Optionally, specify a description for the partition. The description can be up to 1024 characters in length.
   c. For partition type, select **Secure Service Container** from the list, as shown in Figure 5.



New Partition - RACKPR27

Provide a name and description for the partition.

* Name: SSC_Partition

Description:

Partition Type: Secure Service Container

Provide a master user ID and password to use when logging in to the SSC web interface.

* Master User ID:

* Master Password:

* Confirm Master Password:

Figure 5. A portion of the Name page of the New Partition task in basic mode

When the selected partition type is **Secure Service Container**, the page display includes the following additional fields.

Master User ID
Enter the user ID to be used as the default master user ID for the Secure Service Container partition. This user ID has authority to perform any task that is available through the Secure Service Container graphical user interface (GUI).

A master user ID can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: period (.), underscore (_), and hyphen (-).

Master Password
Enter the password for the master user ID. A master password can have a minimum of 8 characters and a maximum of 256 characters. A master password is case-sensitive and can contain numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: hyphen (-), underscore (_), exclamation (!), at (@), hash (#), dollar ($), percent (%), carat (^), ampersand (&), asterisk (*), left parenthesis ((), right parenthesis ()), plus (+), left brace ({), right brace (}), vertical bar (|), colon (:), less than (<), greater than (>), question mark (?), and equals (=).

Confirm Master Password

Reenter the password exactly as you typed it for the Master Password field.

d. When you have finished, click **Next** to navigate to the next page in the task.

3. Required: Use the Processors page to define the number of virtual processors for the partition, and to view various charts that are based on your selections. Select the number of processors that you want to assign to your new partition. Processors can be either shared or dedicated. Although you can select a number of processors greater than the number that is currently available, your new partition will not start unless currently active, unreserved partitions are stopped or more processors are added to the system.

   When you have finished, click **Next** to navigate to the next page in the task.

4. Required: Use the Memory page to define the initial and maximum amounts of memory to be assigned to the new partition.

   When you define the amount of memory to be assigned, or allocated, to a specific partition, you specify an initial amount of memory, and a maximum amount that must be equal to or greater than the initial amount. For a Secure Service Container partition, you must specify a minimum initial amount of 4096 MB (4 GB).

   When you have finished, click **Next** to navigate to the next page in the task.

5. Required: Use the Network page to define all of the network interface cards (NICs) that the new partition requires to access specific networks. For a Secure Service Container partition, you must also specify at least one NIC for communication with the Secure Service Container web interface.

   a. From the Actions list in the NICs table, select **New** to open the New Network Interface Card window.

   b. On the New Network Interface Card window, define a NIC for each network connection that is required for the operating system or hypervisor that runs on this partition, or for the applications that the operating system or hypervisor supports. For each NIC that you define, complete the following steps.

      1) Enter a unique, meaningful name and, optionally, a description of the new NIC.

      2) Set the **Use to access the web interface** switch for each NIC that you are creating. Set the switch to **YES** only for a NIC that provides access to the Secure Service Container web interface.

         When the switch is set to **YES**, the display includes the following configuration settings, which Secure Service Container partitions require for access to the web interface. In addition, DPM filters the entries in the Adapter Ports and Switches table to include only the adapter types that Secure Service Container supports: OSA cards configured to use port 0, and HiperSockets.

         VLAN ID

         Specify the virtual local area network (VLAN) if the link you are using is defined in `TRUNK` mode. The valid range of VLAN IDs is 1 - 4094.

         IP Address Type

         Select one of the following types:
         - **DHCP** (Dynamic Host Configuration Protocol)
         - **Link Local**
         - **Static IPv4 Address**
         - **Static IPv6 Address**

         The selected type determines which of the remaining fields require values. An asterisk (*) preceding the label indicates that a value is required.

         IP Address

         Enter the IP address of the network adapter. This field is required only for IP addresses of type **Static IPv4 Address** and **Static IPv6 Address**.

Mask/Prefix
For an IPv4 address type, enter the mask/prefix in either bit notation (for example, `/24`) or mask notation (for example, `255.255.255.0`). For an IPv6 address type, enter the mask/prefix in bit notation only.

3) Review the entries in the Adapter Ports and Switches table to determine which network adapters are configured on the system. Select only one port or switch by clicking the radio button in the Select column.
4) Click **OK** to create the new NIC and close the New Network Interface Card window.
5) Check the entry for the new NIC that is displayed in the NICs table in the Network section.

If the new NIC provides access to the Secure Service Container web interface, provide the required network settings that are displayed after the NICs table. Some of the values that you supply depend on the IP address type of the NIC that you created to access the web interface. An asterisk (*) preceding the label indicates that a value is required.

Host Name
Enter the Linux host name of the appliance to run in the Secure Service Container partition. To access the Secure Service Container web interface, users need to specify a URL that contains either a host name or an IP address for the Secure Service Container partition. A host name can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (any case), and the following special characters: period (.), colon (:), and hyphen (-).

Default IPv4 Gateway
Enter an IPv4 address for the default gateway, when the IP address type of the NIC is IPv4.

DNS Server 1
Enter an IPv4 or IPv6 address for the primary domain name system (DNS) server. A DNS server definition is required if you specified a Dynamic Host Configuration Protocol (DHCP) IP address for the NIC.

DNS Server 2
Enter an IPv4 or IPv6 address for a secondary DNS server.

c. Repeat the preceding steps, as necessary, to create a new NIC for each network connection that your new partition requires. If you define multiple NICs for a Secure Service Container partition, use the “Use to access the web interface” switch to identify whether the NIC provides access to the web interface.
d. When you have finished, click **Next** to navigate to the next page in the task.

6. Use the Storage page to define host bus adapters (HBAs) to enable the new partition to access specific storage networks and devices.

   For a Secure Service Container partition, the storage requirements depend on the type of appliance that you plan to install in the partition.

   - For a software appliance, define at least one HBA to access the storage device on which the appliance installation image resides.
   - For a firmware appliance, you are not required to define an HBA because access to a storage device is not required to install a firmware appliance.

   a. From the Actions list in the HBAs table, select **New** to open the New Host Bus Adapter window.
   b. On the New Host Bus Adapter window, define an HBA for each storage area network that is required for the applications that run on this partition. For each HBA that you define, complete the following steps.
      1) Enter a unique, meaningful name and, optionally, a description of the new HBA.
      2) Review the entries in the Adapter Ports table to determine which storage adapters are configured on the system. Select one port by clicking the radio button in the Select column.
      3) Click **OK** to create the new HBA and close the New Host Bus Adapter window.

   c. Check the entry for the new HBA that is displayed in the HBAs table in the Storage section. When you have finished, click **Next** to navigate to the next page in the task.

   The next page to open might be either Accelerators, Cryptos, or Boot, depending on the system configuration. If the system does not have any configured accelerators or cryptographic features, the Accelerators or Cryptos page cannot be accessed.

7. If the system has configured accelerators, use the Accelerators page to enable the new partition to use accelerators that it requires. Accelerators are optional features and, therefore, might not be installed on the system.
8. If the system has configured cryptographic features, use the Cryptos page to enable the new partition to use the cryptographic features that it requires. Crypto features are optional and, therefore, might not be installed on the system.
9. On the Boot page, note that option set in the “Boot from” menu is **Secure Service Container**. This boot option cannot be changed unless you first change the partition type.

   With this option, the display includes the **Boot in Installer Mode** switch, which is set to **YES** and cannot be set to **NO**. With the switch set to **YES**, the partition start process initializes the Secure Service Container Installer so you can install an appliance in the partition.
10. Click **Next** to navigate to the Summary page.

    You might need to vertically scroll the Summary page to view all of the partition properties. If necessary, click **Back** to return to a particular page to change a property value or setting.
11. Required: On the Summary page, click **Finish** to save the partition definition. A progress indicator is displayed until DPM finishes creating the partition.

Results

DPM opens the Validation window when it finishes creating the partition definition. The Validation window displays a message indicating that your Secure Service Container partition has been created, and lists additional tasks that you can use to work with the new partition.

When you are finished reviewing the information on the Validation window or using the provided links to related tasks, click **Close** to close the Validation window.

What to do next

Start the Secure Service Container partition by following the instructions in Chapter 9, “Starting a Secure Service Container partition on a DPM-enabled system,” on page 35.

If you need to modify the logon or network settings at a later time, see the instructions in the following topics:

- Chapter 10, “Changing the login settings for a Secure Service Container partition on a DPM-enabled system,” on page 37
- Chapter 11, “Changing the network settings for a Secure Service Container partition on a DPM-enabled system,” on page 39

Chapter 9. Starting a Secure Service Container partition on a DPM-enabled system

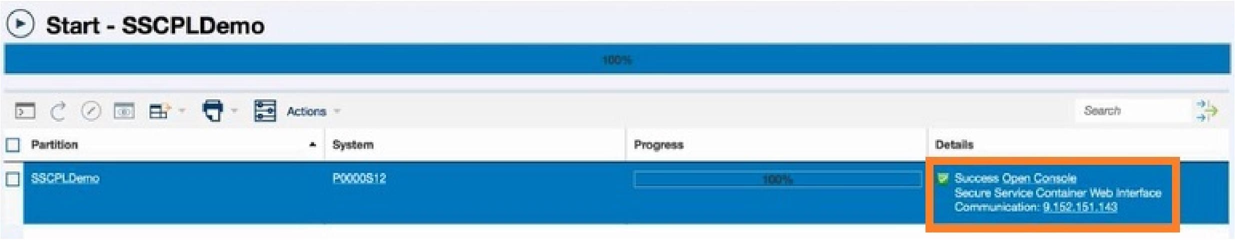
Use this procedure to start a Secure Service Container partition through the Hardware Management Console (HMC) on a host system with IBM Dynamic Partition Manager (DPM) enabled.

Before you begin

- Before activating the Secure Service Container partition, make sure that I/O and storage devices have been configured for this partition through the **Manage Adapters** task. The I/O and storage device requirements depend on the appliance that you plan to install.
- To activate the Secure Service Container partition, make sure that you log in to the HMC with a user ID that is assigned to one of the following roles: SYSPROG, OPERATOR, or ADVANCED.

Procedure

1. Select the image for the Secure Service Container partition.
2. From the **Daily** task group, open the **Start** task. The Start window is displayed. The Start window includes a progress bar, along with information about the start operation in the Progress or Details columns.
3. Check the Details column for the results of the start operation. If it completed successfully, the Details column contains an IP address link that you can use to access the Secure Service Container web interface through a browser. Figure 6 shows the part of the Start task window where the IP address is displayed.



Start - SSCPLDemo

100%

Partition	System	Progress	Details
SSCPLDemo	P0000S12	100%	Success Open Console Secure Service Container Web Interface Communication: 9.152.151.143

Figure 6. Portion of a Start task window with the successful completion indicated in the Details column

4. Click **OK** to close the window when the activation completes successfully.

   Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Results

When the Secure Service Container partition is started, the sequence of events varies, depending on the setting of the **Boot in Installer Mode** switch in the Boot section of the **Partition Details** task.

If the switch is set to YES

The partition start process initializes the Secure Service Container Installer so you can install an appliance. This boot selection is the only option when you start a newly configured Secure Service Container partition for the first time. With this option, the Secure Service Container Installer is started automatically. When the start process completes, you can access the Secure Service Container Installer through your choice of browser. For more instructions, see the appropriate installation topic in Part 4, "Software appliances," on page 43.

© Copyright IBM Corp. 2016, 2017

If the switch is set to NO

With this boot selection, the partition start process effectively restarts an installed appliance. If you previously used the Secure Service Container Installer to successfully install a firmware or software appliance, this boot selection becomes the default selection in the partition definition for the Secure Service Container partition. In this case, the Secure Service Container Installer is rebooted, and the installed appliance is restarted in the Secure Service Container partition on this and all subsequent reboots, until you change the boot selection in the **Partition Details** task.

What to do next

- To find the IP address of the Secure Service Container partition after you close the Start window, select the partition and start the **Operating System Messages** task. In the resulting display, search for the message about connecting to the Secure Service Container installer, which includes the IP address through which the Secure Service Container server is listening.
- If you have started a new Secure Service Container partition for the first time, connect to the Secure Service Container installer through the browser of your choice, and install a software appliance. For instructions, see the appropriate topic in Part 4, “Software appliances,” on page 43.

  If your company has the IBM zAware hardware feature on a supported z Systems or LinuxONE server, you can install IBM zAware in a Secure Service Container partition. For additional details and instructions, see *z Advanced Workload Analysis Reporter (IBM zAware) Guide*, SC27-2632.
- If a previously installed appliance has been restarted, use the IP address to connect to the appliance. For more details, see the product documentation for the installed appliance.

Chapter 10. Changing the login settings for a Secure Service Container partition on a DPM-enabled system

Use this procedure when you need to change the current login settings for a Secure Service Container partition on a host system with IBM Dynamic Partition Manager (DPM) enabled. This procedure is intended for system administrators or system programmers who are responsible for configuring logical partitions on z Systems and LinuxONE servers. To modify the login settings of a Secure Service Container partition, use the Hardware Management Console (HMC) **Partition Details** task to modify the partition definition.

Before you begin

Make sure that you log in to the HMC with a user ID that is assigned to one of the following roles: SYSPROG, ADVANCED, OPERATOR or ACSADMIN.

About this task

A system administrator might need to change the current login settings for the partition, for example, to comply with company rules for changing passwords. An administrator also might change the master ID and password for the partition if the ID and password values are forgotten or lost.

Note that changing the login settings is a disruptive action if the partition status is any value other than **Stopped**.

Procedure

1. From the Systems Management menu on the HMC, select the system on which you created the Secure Service Container partition, and select that partition in the Partitions list.
2. Click the partition name to open the **Partition Details** task.
3. In the **General** section, click **RESET LOGIN**.
   a. Replace the current values for either the default master user ID, the password, or both.

      Master user ID
         Enter the user ID to be used as the default master user ID for the Secure Service Container partition. This user ID has authority to perform any task that is available through the Secure Service Container graphical user interface (GUI).

         A master user ID can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: period (.), underscore (_), and hyphen (-).

      Master password
         Enter the password for the master user ID. A master password can have a minimum of 8 characters and a maximum of 256 characters. A master password is case-sensitive and can contain numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: hyphen (-), underscore (_), exclamation (!), at (@), hash (#), dollar ($), percent (%), carat (^), ampersand (&), asterisk (*), left parenthesis ((), right parenthesis ()), plus (+), left brace ({), right brace (}), vertical bar (|), colon (:), less than (<), greater than (>), question mark (?), and equals (=).

      Confirm master password
         Reenter the password exactly as you typed it for the Master password field.
4. Click **OK** or **Apply** to save your changes.

© Copyright IBM Corp. 2016, 2017

If the partition status is Stopped
Your changes are saved but do not take effect until you start the partition.

If the partition status is any value other than Stopped
The Confirm Disruptive Action window opens. Depending on the type of requested changes, you might be required to type in confirmation text or enter your password. On the **Confirm Disruptive Action** window, complete the following steps to save your changes. Note that they do not take effect until you stop and restart the partition.

a. Review the Changes table to verify the disruptive changes that you requested.

b. Review the Partition table to determine whether you must type a confirmation value. This table contains the following columns:

   Name The name of the partition for which you are requesting disruptive changes.

   System
   The system that is associated with this partition. The system name is a hyperlink through which you can open the **System Details** task.

   Status The current status of this partition.

   OS Name
   The operating system name that is associated with this partition.

   Confirmation Text
   This column is displayed only if you are required to type in confirmation that the action will disrupt a partition's operations. To confirm, type either the value in the Name column, or the value in the OS Name column, exactly as it is displayed in this table.

c. If you are required to enter a password, this display includes a text box in which you need to type the password associated with your user ID.

d. Click **Save** to save the changes that you have requested, or click **Cancel** to close the window without saving any changes.

Results

The partition definition has been updated with the revised login settings.

What to do next

Start the Secure Service Container partition by following the instructions in Chapter 9, “Starting a Secure Service Container partition on a DPM-enabled system,” on page 35.

Chapter 11. Changing the network settings for a Secure Service Container partition on a DPM-enabled system

Use this procedure when you need to change the current network settings for a Secure Service Container partition on a host system with IBM Dynamic Partition Manager (DPM) enabled. This procedure is intended for system administrators or system programmers who are responsible for configuring logical partitions on z Systems and LinuxONE servers. To modify the network settings of a Secure Service Container partition, use the Hardware Management Console (HMC) **Partition Details** task to modify the partition definition.

Before you begin

Make sure that you log in to the HMC with a user ID that is assigned to one of the following roles: SYSPROG, ADVANCED, OPERATOR or ACSADMIN.

About this task

A system administrator might need to change the current network settings for the partition, for example, when the hardware configuration changes or when an additional network is required.

Note that changing the network settings is a disruptive action if the partition status is any value other than **Stopped**.

Procedure

1. From the Systems Management menu on the HMC, select the system on which you created the Secure Service Container partition, and select that partition in the Partitions list.
2. Click the partition name to open the **Partition Details** task.
3. In the **Network** section, click **RESET NETWORK**.
   a. Replace the current values for one or more of the following network settings.

      Host Name
      Enter the Linux host name of the appliance to run in the Secure Service Container partition. To access the Secure Service Container web interface, users need to specify a URL that contains either a host name or an IP address for the Secure Service Container partition. A host name can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (any case), and the following special characters: period (.), colon (:), and hyphen (-).

      Default IPv4 Gateway
      Enter an IPv4 address for the default gateway, when the IP address type of the NIC is IPv4.

      DNS Server 1
      Enter an IPv4 or IPv6 address for the primary domain name system (DNS) server. A DNS server definition is required if you specified a Dynamic Host Configuration Protocol (DHCP) IP address for the NIC.

      DNS Server 2
      Enter an IPv4 or IPv6 address for a secondary DNS server.
4. Click **OK** or **Apply** to save your changes.

   If the partition status is Stopped
   Your changes are saved but do not take effect until you start the partition.

© Copyright IBM Corp. 2016, 2017

If the partition status is any value other than Stopped

The Confirm Disruptive Action window opens. Depending on the type of requested changes, you might be required to type in confirmation text or enter your password. On the **Confirm Disruptive Action** window, complete the following steps to save your changes. Note that they do not take effect until you stop and restart the partition.

a. Review the Changes table to verify the disruptive changes that you requested.

b. Review the Partition table to determine whether you must type a confirmation value. This table contains the following columns:

   Name The name of the partition for which you are requesting disruptive changes.

   System
   The system that is associated with this partition. The system name is a hyperlink through which you can open the **System Details** task.

   Status The current status of this partition.

   OS Name
   The operating system name that is associated with this partition.

   Confirmation Text
   This column is displayed only if you are required to type in confirmation that the action will disrupt a partition's operations. To confirm, type either the value in the Name column, or the value in the OS Name column, exactly as it is displayed in this table.

c. If you are required to enter a password, this display includes a text box in which you need to type the password associated with your user ID.

d. Click **Save** to save the changes that you have requested, or click **Cancel** to close the window without saving any changes.

Results

The partition definition has been updated with the revised network settings.

What to do next

Start the Secure Service Container partition by following the instructions in Chapter 9, “Starting a Secure Service Container partition on a DPM-enabled system,” on page 35.

Chapter 12. Stopping or deleting a Secure Service Container partition on a DPM-enabled system

Use this procedure to stop or delete a Secure Service Container partition through the Hardware Management Console (HMC) on a host system with IBM Dynamic Partition Manager (DPM) enabled. This action is a disruptive task.

Before you begin

To stop or delete the Secure Service Container partition, make sure that you log in to the HMC with a user ID that is assigned to one of the following roles: SYSPROG, OPERATOR, or ADVANCED.

About this task

When you determine that you no longer need a Secure Service Container partition, stop and then either delete or modify its partition definition to avoid inadvertently restarting a firmware or software appliance from a disk that might be in use by another partition.

Procedure

1. To stop a Secure Service Container partition, complete the following steps.

   This task stops the installed application and the embedded operating system, and deallocates resources for the selected partition.

   a. Select the image for the Secure Service Container partition.

   b. Open the **Stop** task. The Confirm Disruptive Action window opens.

   c. On the **Confirm Disruptive Action** window, complete the following steps to save your changes.

      1) Review the Changes table to verify the disruptive changes that you requested.

      2) Review the Partition table to determine whether you must type a confirmation value. This table contains the following columns:

         Name The name of the partition for which you are requesting disruptive changes.

         System
         The system that is associated with this partition. The system name is a hyperlink through which you can open the **System Details** task.

         Status The current status of this partition.

         OS Name
         The operating system name that is associated with this partition.

         Confirmation Text
         This column is displayed only if you are required to type in confirmation that the action will disrupt a partition's operations. To confirm, type either the value in the Name column, or the value in the OS Name column, exactly as it is displayed in this table.

      3) If you are required to enter a password, this display includes a text box in which you need to type the password associated with your user ID.

      4) Click **Stop Partition**.

      The Stop window opens to indicate the progress of the stop operation and the outcome.

   d. Click **OK** to close the window when the stop operation completes successfully.

      Otherwise, if the deactivation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

© Copyright IBM Corp. 2016, 2017

2. After the partition is stopped, you can either delete or modify its partition definition to prevent the automatic restart of the partition and its installed application.
   - To delete the partition definition:
     a. Select the image for the Secure Service Container partition.
     b. Open the **Delete Partition** task.
     c. Click **Delete**. The HMC displays a message indicating the status of the delete operation.
   - To modify the partition definition:
     a. Select the image for the Secure Service Container partition.
     b. Open the **Partition Details** task.
     c. On the Boot page, set the **Boot in Installer Mode** switch to **YES**.
     d. Click **OK** to save your changes and close the Partition Details window.

Results

The partition definition is either deleted or modified such that an application cannot be inadvertently restarted in the Secure Service Container partition.

The appliance installation image continues to reside on the storage device, and you can use the Secure Service Container Installer to migrate it to a different partition. Or, if the partition definition still exists, you can change the boot setting to restart the application.

Part 4. Software appliances

This part contains step-by-step instructions for installing software appliances in a Secure Service Container partition.

- Chapter 13, “Installing a new software appliance in a Secure Service Container partition,” on page 45
- Chapter 14, “Using the Secure Service Container user interface,” on page 49
- Chapter 15, “Moving an existing software appliance into a different Secure Service Container partition,” on page 53

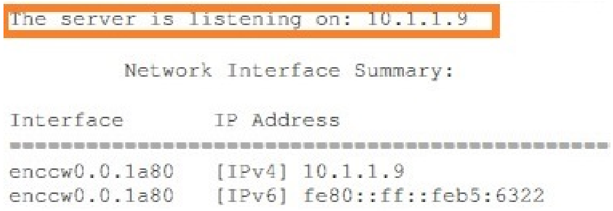
© Copyright IBM Corp. 2016, 2017

Chapter 13. Installing a new software appliance in a Secure Service Container partition

Use this procedure to install and start a new software appliance in a Secure Service Container partition. Only one appliance can be installed and run in a Secure Service Container partition at any given time; this type of partition does not support running multiple appliances simultaneously. You can define more than one Secure Service Container partition on the same system, and run instances of the same appliance in each one. In this case, each partition must use separate storage devices.

Before you begin

- If you plan to install a software appliance on an FCP disk, make sure that your installation has completed the required steps in Chapter 2, “Prerequisites for using Secure Service Container,” on page 7 to enable N Port Identifier Virtualization (NPIV). Target FCP disks must be large enough to fit the uncompressed appliance, with an additional 2 GB for the Secure Service Container installer to use.
- You must configure and start a Secure Service Container partition with the boot option **Secure Service Container Installer** selected. For instructions, see the following topics:
  - On a standard mode system:
    - Chapter 3, “Configuring a Secure Service Container partition on a standard mode system,” on page 13
    - Chapter 4, “Starting a Secure Service Container partition on a standard mode system,” on page 19
  - On a DPM-enabled system:
    - Chapter 8, “Creating a Secure Service Container partition on a DPM-enabled system,” on page 29
    - Chapter 9, “Starting a Secure Service Container partition on a DPM-enabled system,” on page 35
- You need to know the IP address for the Secure Service Container partition. Use the IP address of the network adapter that is specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition. If you do not know the IP address to use, select the partition and start the **Operating System Messages** task. In the resulting display, search for the message about connecting to the Secure Service Container installer, which includes the IP address through which the Secure Service Container server is listening. Figure 7 shows a sample operating system message that contains the IP address.



```
The server is listening on: 10.1.1.9

         Network Interface Summary:

Interface        IP Address
===============================================
enccw0.0.1a80    [IPv4] 10.1.1.9
enccw0.0.1a80    [IPv6] fe80::ff::feb5:6322
```

Figure 7. Sample display of Operating System Messages

- You need to know the master user ID and password for the Secure Service Container partition. These values are specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition.
- Order and download the software appliance to your local disk. For a list of supported appliances, see Chapter 2, “Prerequisites for using Secure Service Container,” on page 7.

Procedure

1. Connect to the Secure Service Container installer through the browser of your choice.

© Copyright IBM Corp. 2016, 2017

Use the IP address of the network adapter that is specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition. For example: `https://ip_address`

You are connected through a Secure Sockets Layer (SSL) connection. If prompted by your browser, accept the self-signed certificate for the SSL connection.

2. On the Login page, enter the master user ID and password values that you supplied in the image profile (standard mode system) or the partition definition (DPM-enabled system), and click **Login**. The main page of the installer opens.
3. On the main page, click the plus (+) icon to install image files from local media. The page display changes to the Install Software Appliance page.
4. On the Install Software Appliance page, complete the following steps.
   a. Make sure that **Upload image to target disk** is selected.
   b. Under Local Installation Image, click Browse and navigate to the location where you installed the software appliance on your local disk. Select the software appliance image and click **Open**. The Image Details section is populated with information about the selected software appliance.
   c. Under Target Disk on Server, select the device type.

      FICON DASD
      If you select **FICON DASD** as the device type, click the down arrow in the **Disk** field to display a list of available disks on the server, and either scroll the list or begin typing a disk name in the text box to filter the search. From the list, select a disk.

      FCP If you select **FCP** as the device type, select one of the options listed for the **Discovery** field.

      Scan All Devices
      Select this option and click **Discover**. When the discovery operation completes, select a disk from the **Disk** list.

      Scan Single Device Only
      Select this option, then select a storage device from the **Device** list, and click **Discover**. When the discovery operation completes, select a disk from the **Disk** list.

      Manual
      Select this option, select a storage device from the **Device** list, and enter the target worldwide port number (WWPN) and logical unit number (LUN) information for the disk. Then click **Check Path** to validate these details. If an error message is displayed, you must correct the WWPN or LUN details before you can proceed.
   d. Click **Apply** to upload the software appliance image to the target disk on the server.

   A confirmation dialog is displayed.
5. On the confirmation dialog, complete the following steps.
   a. Click **Reboot** to have the installer automatically reactivate the partition.
   b. Click **Yes** to continue with the installation.

   The Secure Service Container installer uploads the appliance image to the target disk, and prepares the partition to load the appliance after the next reboot.
   a. When the reboot process begins, the installer displays the Reboot window.
   b. If an IP address type other than DHCP is in use for the appliance page, the Secure Service Container installer redirects the browser to the software appliance page.
6. On the appliance page, complete the following steps.
   a. If prompted by your browser, accept the self-signed certificate for the SSL connection.

b. Enter the master user ID and password values that you supplied in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition, and click **Login**.

Results

The software appliance is available for use. See the product documentation for the appliance for additional information and instructions.

What to do next

You can reuse an existing Secure Service Container partition for a different appliance. After stopping the installed appliance and the partition, reboot the Secure Service Container installer and select a different appliance to install. Before doing so, however, check the storage and network connections for the partition to make sure that they are appropriate for the appliance to be installed.

Chapter 14. Using the Secure Service Container user interface

Appliances that are designed to run in a Secure Service Container partition can use one or more Secure Service Container user interface (UI) widgets, through which you can view the Secure Service Container partition network and logon settings, request a dump of partition data for reporting a problem to IBM, and complete additional management tasks.

To access the installed appliance and view the Secure Service Container UI widgets:

- You need to know the IP address for the Secure Service Container partition. Use the IP address of the network adapter that is specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition.
- You need to know the master user ID and password for the Secure Service Container partition. These values are specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition.

The following list contains brief descriptions of the available UI widgets and the icons that are displayed in the navigation bar.

1. The Dumps widget (⊕) provides the controls through which you can view dumps that have been collected, request a dump, or download the contents of a dump. For more information, see “Requesting and downloading dumps” on page 50.
2. The Log widget (▤) contains a table display of entries that you can use for problem diagnosis. Each log entry indicates the date and time of the entry, the severity and type of the log entry, and the log entry text. If any additional debug information is available, a download icon (⤓) is displayed for the entry; to access this information, click the download icon.

   You can filter the log entries that are displayed on the Log page; the filter text string is matched against the Entry Text field contents. You can also archive log entries, which only removes them from the Log page display. To archive existing log entries, click the file cabinet icon (▭). To retrieve archived logs, request a dump through the Dumps widget.
3. The Ex-/Import widget (⇪) provides controls through which users can export or import appliance data. For more information, see “Exporting or importing appliance configuration data” on page 51.
4. The Networks widget (☍) displays the status and details for the network interfaces that are defined in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition. These details reflect the network information that an administrator specified when defining the partition.
   - For a host system running in standard mode, network details are specified in the image profile of the Secure Service Container partition. To view or modify network information, use the **Customize/Delete Activation Profiles** task.
   - For a host system with DPM enabled, network details are specified in the partition definition. To view or modify network information, use the **Partition Details** task.
5. The Storage widget (▤) displays the current storage settings.
   - For a host system running in standard mode (that is, with Processor Resource/System Manager or PR/SM), storage details are specified in the input/output configuration data set (IOCDS) that is in effect for the host system. To view this information, select the host system under the **System Management** node, expand the **Partitions** node, expand the entry for the Secure Service Container partition, and select **CHPIDs**.

© Copyright IBM Corp. 2016, 2017

- For a host system with IBM Dynamic Partition Manager (DPM) enabled, storage details are specified in the partition definition. To view or modify storage information, use the **Partition Details** task.

Requesting and downloading dumps

Use this procedure to request and download a dump of data for an appliance that is installed and running in a Secure Service Container partition. You can use this function only if the installed appliance is designed to use the Secure Service Container Dump widget.

Before you begin

You can access the Secure Service Container user interface (UI) through the browser of your choice. To access the Secure Service Container UI:

- You need to know the IP address for the Secure Service Container partition. Use the IP address of the network adapter that is specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition.
- You need to know the master user ID and password for the Secure Service Container partition. These values are specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition.

Procedure

1. In the navigation pane, click the **Dumps** icon (⌖) to display the Dumps page.

   The Dumps table lists the dumps, if any, that have been collected. The entry for each dump includes a user-supplied reason for the dump request, and indicates the date and time when the dump content was collected. The dump content is configured by the appliance vendor and is encrypted to protect appliance data.

   To filter the entries in the Dumps table, enter a text string in the Filter text area. If the text string matches text in any of the Dump Reason column entries, the table display includes only matching entries. To clear the filter, click the **x** in the Filter field or delete the text in that field.

2. To request a dump, click the **Add** icon (⊕) to display the Dump dialog.

   a. Select the type of dump that you want.

      Concurrent Dump
      While dump data is collected, the appliance continues to run but some functions might not work as expected.

      Disruptive Dump
      Dump data is collected and the appliance is rebooted.

   b. In the Dump Reason text area, enter information that describes why you are requesting the dump.

   c. Click **Create Dump** to submit the dump request. The resulting process varies, depending on the type of dump you requested.

   For a concurrent dump
   The Dumps table is updated to display a temporary entry for the concurrent dump. The entry includes a status icon. When the dump process is completed, the temporary entry is updated with permanent information for this dump request.

   For a disruptive dump
   The browser display changes to the Reboot page, which changes to the Login page when the appliance has completed the dump and reboot process.

3. To download a specific dump, click the download icon (⤓) in the Dump Date/Time column.

Exporting or importing appliance configuration data

Use this procedure to export or import configuration data for an appliance that is installed and running in a Secure Service Container partition. An administrator might use these functions to update an appliance or to transfer the appliance configuration to another Secure Service Container partition. You can use this function only if the installed appliance is designed to use the Secure Service Container Ex-/Import widget.

Before you begin

You can access the Secure Service Container user interface (UI) through the browser of your choice.

To access the Secure Service Container UI:

- You need to know the IP address for the Secure Service Container partition. Use the IP address of the network adapter that is specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition.
- You need to know the master user ID and password for the Secure Service Container partition. These values are specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition.

Procedure

1. In the navigation pane, click the **Ex-/Import** icon (⇪).
2. To export configuration data for an appliance, complete the following steps.
   a. Click **Export**.
   b. In the Description text area, enter information that describes the appliance or its configuration data.
   c. Click **Export** again.
   d. When prompted by your browser, select **Save File** and click **OK**.

   The configuration file, export.data, is stored in your file system.
3. To import previously exported configuration data, complete the following steps.
   a. Click **Import**.
   b. On the File Upload page, select the export.data file and click **Open**.
   c. On the Confirm Upload page, click **Yes** to continue the upload. The Reboot page is displayed as the appliance configuration data is uploaded.
   d. When the appliance has been rebooted, the Login page is displayed. If the Login page does not appear, refresh your browser or clear its cache; otherwise, start a new browser session.
   e. On the Login page, enter your credentials and click **Login**.

Chapter 15. Moving an existing software appliance into a different Secure Service Container partition

Use this procedure to move an existing software appliance from one Secure Service Container partition to a new Secure Service Container partition. This action is a disruptive task. Only one appliance can be installed and run in a Secure Service Container partition at any given time; this type of partition does not support running multiple appliances simultaneously. You can define more than one Secure Service Container partition on the same system, and run instances of the same appliance in each one. In this case, each partition must use separate storage devices.

Before you begin

- If you plan to install a software appliance on an FCP disk, make sure that your installation has completed the required steps in Chapter 2, “Prerequisites for using Secure Service Container,” on page 7 to enable N Port Identifier Virtualization (NPIV). Target FCP disks must be large enough to fit the uncompressed appliance, with an additional 2 GB for the Secure Service Container installer to use.
- You must configure and start a Secure Service Container partition with the boot option **Secure Service Container Installer** selected. For instructions, see the following topics:
  - On a standard mode system:
    - Chapter 3, “Configuring a Secure Service Container partition on a standard mode system,” on page 13
    - Chapter 4, “Starting a Secure Service Container partition on a standard mode system,” on page 19
  - On a DPM-enabled system:
    - Chapter 8, “Creating a Secure Service Container partition on a DPM-enabled system,” on page 29
    - Chapter 9, “Starting a Secure Service Container partition on a DPM-enabled system,” on page 35
- You need to know the IP address for the Secure Service Container partition. Use the IP address of the network adapter that is specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition. If you do not know the IP address to use, select the partition and start the **Operating System Messages** task. In the resulting display, search for the message about connecting to the Secure Service Container installer, which includes the IP address through which the Secure Service Container server is listening.
- You need to know the master user ID and password for the Secure Service Container partition. These values are specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition.
- You need to know the ID of the disk on which the existing software appliance image is currently installed. This disk must be attached to the server that hosts the new Secure Service Container partition.

Procedure

1. Connect to the Secure Service Container installer through the browser of your choice.

   Use the IP address of the network adapter that is specified in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition. For example: `https://`*`ip_address`*

   You are connected through a Secure Sockets Layer (SSL) connection. If prompted by your browser, accept the self-signed certificate for the SSL connection.
2. On the Login page, enter the master user ID and password values that you supplied in the image profile (standard mode system) or the partition definition (DPM-enabled system), and click **Login**. The main page of the installer opens.

© Copyright IBM Corp. 2016, 2017

3. On the main page, click the plus (+) icon to install image files from local media. The page display changes to the Install Software Appliance page.
4. On the Install Software Appliance page, complete the following steps.
   a. Select **Attach existing disk**.
   b. In the Existing Disk with Software Appliance section, select the device type.

      FICON DASD
      If you select **FICON DASD** as the device type, click the down arrow in the **Disk** field to display a list of the disks attached to the server, and either scroll the list or begin typing a disk name in the text box to filter the search. From the list, select the disk on which the software appliance resides.

      FCP If you select **FCP** as the device type, select one of the options listed for the **Discovery** field.

      Scan All Devices
      Select this option and click **Discover**. When the discovery operation completes, select the disk on which the software appliance resides from the **Disk** list.

      Scan Single Device Only
      Select this option, then select a storage device from the **Device** list, and click **Discover**. When the discovery operation completes, select the disk on which the software appliance resides from the **Disk** list.

      Manual
      Select this option, select a storage device from the **Device** list, and enter the target worldwide port number (WWPN) and logical unit number (LUN) information for the disk on which the software appliance resides.

      The Image Details section is populated with information about the software appliance.
   c. Click **Apply** to install and start the software appliance.

   A confirmation dialog is displayed.
5. On the confirmation dialog, complete the following steps.
   a. Click **Reboot** to have the installer automatically reactivate the partition.
   b. Click **Yes** to continue with the installation.

   The Secure Service Container installer attaches the selected disk, and prepares the partition to load the appliance after the next reboot.
   a. When the reboot process begins, the installer displays the Reboot window.
   b. If an IP address type other than DHCP is in use for the appliance page, the Secure Service Container installer redirects the browser to the software appliance page.
6. On the appliance page, complete the following steps.
   a. If prompted by your browser, accept the self-signed certificate for the SSL connection.
   b. Enter the master user ID and password values that you supplied in the image profile (standard mode system) or the partition definition (DPM-enabled system) for the Secure Service Container partition, and click **Login**.

Results

The software appliance is available for use. See the product documentation for the appliance for additional information and instructions.

Part 5. Appendixes

© Copyright IBM Corp. 2016, 2017

Appendix. Notices

This information was developed for products and services offered in the US.

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

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.

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-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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

© Copyright IBM Corp. 2016, 2017

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 enterprise is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com® are 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.

Linux is a registered trademark of Linux 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.

Class A Notices

The following Class A statements apply to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

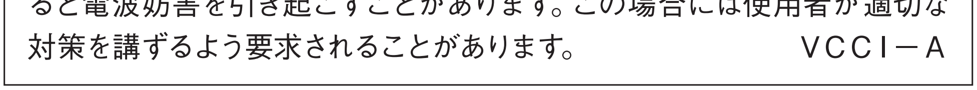
This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55032. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Statement - Japan

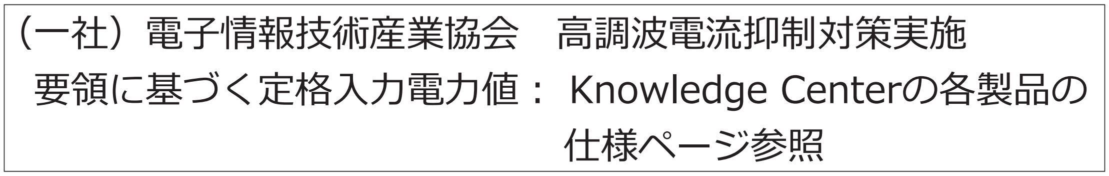


この装置は，クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　ＶＣＣＩ－Ａ

The following is a summary of the Japanese VCCI statement above:

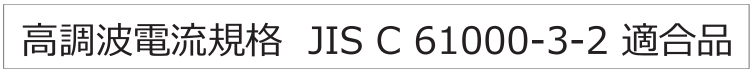
This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Japan JIS C 61000-3-2 Compliance



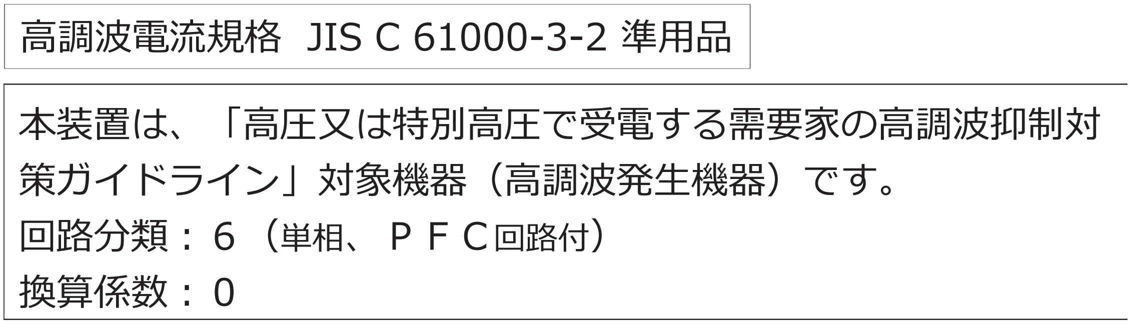
（一社）電子情報技術産業協会　高調波電流抑制対策実施要領に基づく定格入力電力値：Knowledge Centerの各製品の仕様ページ参照

For products less than or equal to 20 A per phase, the following statement applies:



高調波電流規格 JIS C 61000-3-2 適合品

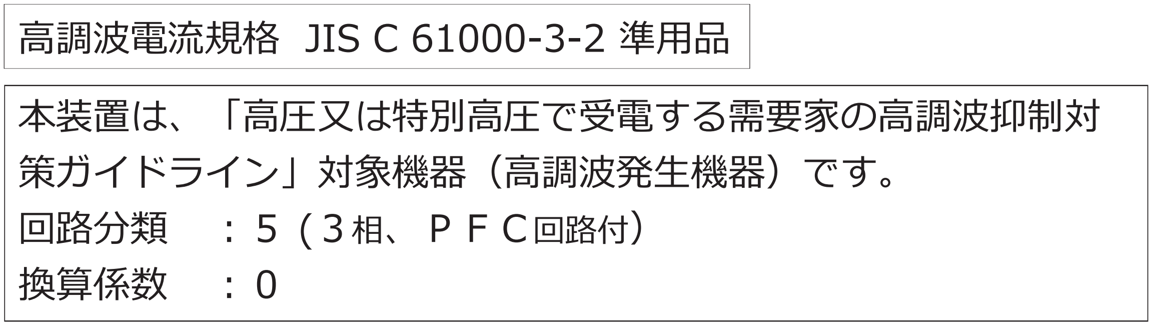
For products greater than 20 A, single-phase, the following statements apply:



高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
回路分類：6（単相、ＰＦＣ回路付）
換算係数：0

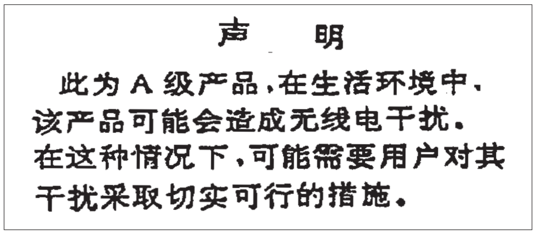
For products greater than 20 A per phase, three-phase, the following statements apply:



高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
回路分類　：5（3相、ＰＦＣ回路付）
換算係数　：0

Electromagnetic Interference (EMI) Statement - People's Republic of China

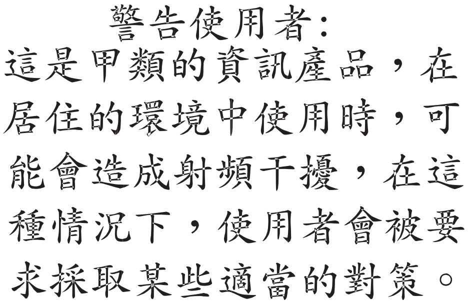


声　明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Declaration: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may need to perform practical action.

Electromagnetic Interference (EMI) Statement - Taiwan

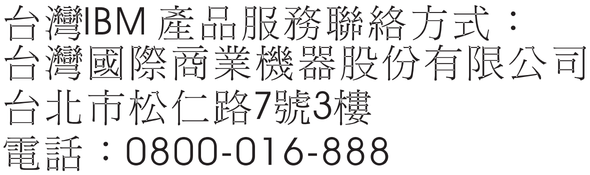


警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

The following is a summary of the Taiwan EMI statement above:

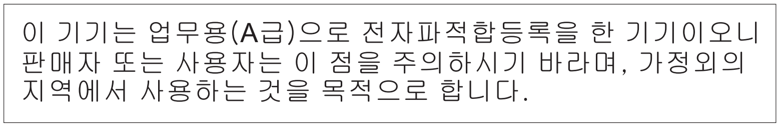
Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user will be required to take adequate measures.

IBM Taiwan Contact Information:



台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea



이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2014/30/EU) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

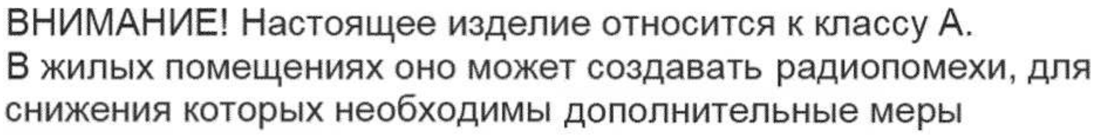
Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH

Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia



ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для
снижения которых необходимы дополнительные меры

Index

A

accessibility x
- contact IBM x
- features x

activate
- Secure Service Container partition
  - on PR/SM 19

Activate task 19

appliance
- definition 3
- install existing 53
- install new 45

appliance configuration data
- export or import 51

assistive technologies x

C

change
- logon settings 21, 37
- master ID and password 21, 37
- network settings 39
  - on PR/SM 23

configure
- Secure Service Container partition
  - on DPM 29
  - on PR/SM 13

create
- Secure Service Container partition
  - on DPM 29
  - on PR/SM 13

Customize/Delete Activation Profiles task 13, 21, 23

Customize/Delete Image Profile task 25

D

deactivate
- Secure Service Container partition
  - on DPM 41
  - on PR/SM 25

delete
- Secure Service Container partition
  - on DPM 41
  - on PR/SM 25

download
- dump 50

DPM
- host system mode 7, 29

DPM-enabled
- host system mode 3

dump
- download 50
- request 50

Dynamic Partition Manager
- *See* DPM

E

ECKD storage
- prerequisites 8

engineering change 7

export
- appliance configuration data 51

Extended Count Key Data storage
- *See* ECKD storage

F

FCP disks
- prerequisites 8

Fibre Channel Protocol disks
- *See* FCP disks

firmware appliance
- definition 3
- IBM zAware 13

H

Hardware Management Console
- *See* HMC

HMC
- Activate task 19
- Customize/Delete Activation Profiles task 13, 21, 23
- Customize/Delete Image Profile task 25
- New Partition task 29
- Partition Details task 37, 39
- Start task 35
- Stop task 41

host system mode
- DPM 7, 29
- DPM-enabled 3
- PR/SM 7
- standard (PR/SM) 3, 13, 19, 21, 23

I

IBM Blockchain High Security Business Network 9

IBM Dynamic Partition Manager
- *See* DPM

IBM zAware 9, 13

import
- appliance configuration data 51

install existing appliance 53

install new appliance 45

K

keyboard
- navigation x

L

logical partition
- definition 3

logon settings
- for a Secure Service Container partition 13, 29
  - on DPM 37
  - on PR/SM 21
- view in Secure Service Container UI 49

M

master ID and password 21, 37

microcode control level (MCL) 7

migrate
- existing appliance 53

modify
- logon settings
  - on DPM 37
  - on PR/SM 21
- master ID and password 21, 37
- network settings
  - on DPM 39
  - on PR/SM 23

move
- existing appliance 53

N

N Port Identifier Virtualization
- *See* NPIV

navigation
- keyboard x

network settings
- for a Secure Service Container partition 13, 29
  - on DPM 39
  - on PR/SM 23
- view in Secure Service Container UI 49

New Partition task 29

NPIV
- steps to enable 8

P

partition
- *See* Secure Service Container partition

Partition Details task 37, 39

PR/SM
- host system mode 3, 7, 13, 19, 21, 23

prerequisites
- for using Secure Service Container 7

Processor Resource/System Manager
- *See also* (PR/SM
- *See* PR/SM

© Copyright IBM Corp. 2016, 2017

R

request
  dump 50
revisions xiii

S

Secure Service Container
  definition 3
  prerequisites 7
  value 3
Secure Service Container installer
  install existing appliance 53
  install new appliance 45
Secure Service Container partition
  changing logon settings
    on DPM 37
    on PR/SM 21
  changing network settings
    on DPM 39
    on PR/SM 23
  configuring
    on DPM 29
    on PR/SM 13
  creating
    on DPM 29
    on PR/SM 13
  definition 3
  on DPM
    deleting 41
    stopping 41
  on PR/SM
    deactivating 25
    deleting 25
  set logon values 13, 29
  set network values 13, 29
  starting
    on DPM 35
    on PR/SM 19
  user interface 49
Secure Service Container user interface (UI) 49
  export or import appliance configuration data 51
  request or download dumps 50
settings
  for a Secure Service Container partition
    logon 13, 21, 29, 37
    network 13, 23, 29, 39
shortcut keys x
software appliance
  definition 3
standard mode (PR/SM)
  host system mode 3, 13, 19, 21, 23
start
  Secure Service Container partition
    on DPM 35
    on PR/SM 19, 25
Start task 35
stop
  Secure Service Container partition
    on DPM 41
Stop task 41
storage devices
  supported types 8

Z

z/VSE Network Appliance (VNA) 9

Printed in USA

SC28-6971-01