IBM Z and LinuxONE

Secure Service Container User's Guide

SC28-7062-00

Note:

Before you use this information and the product it supports, read the information in "Safety" on page ix, Appendix C, "Notices," on page 73 and *IBM Systems Environmental Notices and User Guide*, Z125–5823.

This edition, SC28-7062-00, applies to IBM Z and IBM LinuxONE (LinuxONE) servers.

There might be a newer version of this document available on **IBM Documentation**. Go to https://www.ibm.com/docs/en/systems-hardware, select **IBM Z** or **IBM LinuxONE**, then select your configuration, and click **Library Overview** on the navigation bar.

Contents

Figures

Tables

Safety

Safety notices

Safety notices may be printed throughout this document. **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.

DANGER notices:

DANGER: To prevent a possible shock from touching two surfaces with different protective ground (earth), use one hand, when possible, to connect or disconnect signal cables. (D001)

DANGER: If the receptacle has a metal shell, do not touch the shell until you have completed the voltage and grounding checks. Improper wiring or grounding could place dangerous voltage on the metal shell. If any of the conditions are not as described, *STOP*. Ensure the improper voltage or impedance conditions are corrected before proceeding. (D003)

DANGER: An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (D004)

DANGER: Heavy equipment — personal injury or equipment damage might result if mishandled. (D006)

DANGER: When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard: If IBM supplied the power cord(s), connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product. Do not open or service any power supply assembly. Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.

-  The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords. For AC power, disconnect all power cords from their AC power source. For racks with a DC power distribution panel (PDP), disconnect the customer's DC power source to the PDP.
- When connecting power to the product ensure all power cables are properly connected. For racks with AC power, connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate. For racks with a DC power distribution panel (PDP), connect the customer's DC power source to the PDP. Ensure that the proper polarity is used when attaching the DC power and DC power return wiring.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Do not attempt to switch on power to the machine until all possible unsafe conditions are corrected.
- When performing a machine inspection: Assume that an electrical safety hazard is present. Perform all continuity, grounding, and power checks specified during the subsystem installation procedures to ensure that the machine meets safety requirements. Do not attempt to switch power to the machine until all possible unsafe conditions are corrected. Before you open the device covers, unless instructed otherwise in the installation and configuration procedures: Disconnect the attached AC power cords,

turn off the applicable circuit breakers located in the rack power distribution panel (PDP), and disconnect any telecommunications systems, networks, and modems.

- Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.

  To Disconnect: 1) Turn off everything (unless instructed otherwise). 2) For AC power, remove the power cords from the outlets. 3) For racks with a DC power distribution panel (PDP), turn off the circuit breakers located in the PDP and remove the power from the Customer's DC power source. 4) Remove the signal cables from the connectors. 5) Remove all cables from the devices.

  To Connect: 1) Turn off everything (unless instructed otherwise). 2) Attach all cables to the devices. 3) Attach the signal cables to the connectors. 4) For AC power, attach the power cords to the outlets. 5) For racks with a DC power distribution panel (PDP), restore the power from the Customer's DC power source and turn on the circuit breakers located in the PDP. 6) Turn on the devices.

-  Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching. (D005)

CAUTION notices:

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)

CAUTION: The doors and covers to the product are to be closed at all times except for service by trained service personnel. All covers must be replaced and doors locked at the conclusion of the service operation. (C013)

CAUTION: Ensure the building power circuit breakers are turned off BEFORE you connect the power cord or cords to the building power. (C023)

CAUTION: The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.
Do not: Throw or immerse into water, heat to more than 100°C (212°F), repair or disassemble. (C003)

 **CAUTION:** This equipment is not suitable for use in locations where children are likely to be present. (C052)

World trade safety information

Several countries require the safety information contained in product publications to be provided in their local language(s). 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 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® and IBM LinuxONE (LinuxONE) models can use I/O cards such as FICON®, Open Systems Adapter (OSA), Network Express, Integrated Coupling Adapter2.0 SR (ICA SR2.0), zHyperLink Express, 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.

Laser Notice: U.S. FDA CDRH NOTICE if low power lasers are utilized, integrated, or offered with end product systems as applicable. Complies with 21 CFR 1040.10 and 1040.11 except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019.

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)

About this publication

This book describes how to use the Secure Service Container to install and run software appliances on IBM Z and 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.

You can configure Secure Service Container partitions on the following systems:

- IBM z17: machine types 9175 and 9176
- IBM z16™: machine types 3931 and 3932
- IBM z15®: machine types 8561 and 8562
- IBM LinuxONE Rockhopper (Rockhopper V)
- IBM LinuxONE Emperor V (Emperor V)
- IBM LinuxONE Emperor 4: machine type 3931
- IBM LinuxONE Rockhopper 4: machine type 3932
- IBM LinuxONE III: machine types 8561 and 8562

This book describes the version of Secure Service Container that is available starting with the Hardware Management Console (HMC) / Support Element (SE) Version 2.17.0.

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 Secure Service Container partition.

Prerequisite and related information

To create and manage Secure Service Container partitions, system administrators use specific tasks on the HMC for a host system running either in standard mode (that is, with Processor Resource/System Manager or PR/SM), or with Dynamic Partition Manager (DPM) enabled. These HMC tasks can be accomplished through a program as well, with the HMC Web Services application programming interfaces (APIs).

- For more information about the host system, see the appropriate overview on the IBM Redbooks® website at http://www.redbooks.ibm.com/. For example, for the IBM z17, see the *IBM z17 Technical Introduction*, SG24-8580.
- The following related publications are available on **IBM Documentation**. Go to https://www.ibm.com/docs/en/systems-hardware, select **IBM Z** or **IBM LinuxONE**, then select your configuration, and click **Library Overview** on the navigation bar.
  - For more information about PR/SM, see *PR/SM Planning Guide*.
  - For information about DPM, see *IBM Dynamic Partition Manager Guide*.
  - For information about the HMC APIs, see *Hardware Management Console Web Services API*.

HMC users also can monitor and manage systems and partitions through the IBM® HMC Mobile (HMC Mobile) mobile app for iOS and Android. The systems can either run in standard mode (that is, with Processor Resource/System Manager or PR/SM), or run with DPM enabled. The HMC Mobile app provides system and partition views, status monitoring, hardware messages, operating system messages, and the ability to receive push notifications from the HMC, using the existing support server connection. For more information, see the HMC online help for the **HMC Mobile Settings** task.

Related HMC and SE console information

Hardware Management Console (HMC) and Support Element (SE) information can be found on the console help system.

How to use this publication

This book provides an overview of the 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.

Topics are organized into the following parts.

Part 1, "Introduction to the Secure Service Container ," on page 1
Topics in this part contain general information about Secure Service Container and the advantages of installing software appliances in a Secure Service Container partition, and the prerequisites for use.

Part 2, "Working with Secure Service Container partitions on a standard mode system," on page 11
Topics in this part contain 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).

Part 3, "Working with Secure Service Container partitions on a DPM-enabled system," on page 27
Topics in this part contain step-by-step instructions for initially configuring and starting a Secure Service Container partition on a host system with DPM enabled.

Part 4, "Software appliances," on page 43
Topics in this part contain step-by-step instructions for installing software appliances in a Secure Service Container partition, using the Secure Service Container user interface, and moving an existing appliance to another Secure Service Container partition.

Appendixes
Topics in this part include error and information codes from the Secure Service Container installer, legal notices, and trademarks.

Accessibility features

Accessibility features help users who have physical disabilities such as restricted mobility or limited vision use software products successfully. The accessibility features can help users do the following tasks:

- Run assistive technology such as screen readers and screen magnifier software.
- Operate specific or equivalent features by using the keyboard.
- Customize display attributes such as color, contrast, and font size.

Consult assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in this product. Consult the product information for the specific assistive technology product that is used to access our product information.

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 provide feedback to IBM

We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

For additional information use the following link that corresponds to your configuration:

Configuration	Link
IBM z17® Model ME1	How to send feedback to IBM
IBM LinuxONE Emperor 5 Model ML1	How to send feedback to IBM

Part 1. Introduction to the Secure Service Container

This part contains general information about 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

The IBM Secure Service Container is a container technology through which you can more quickly and securely deploy software appliances on IBM Z and IBM LinuxONE (LinuxONE) servers. A Secure Service Container partition is a specialized container for installing and running specific 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.

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 I/O adapters.

IBM Z 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 how an administrator defines 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 3 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.

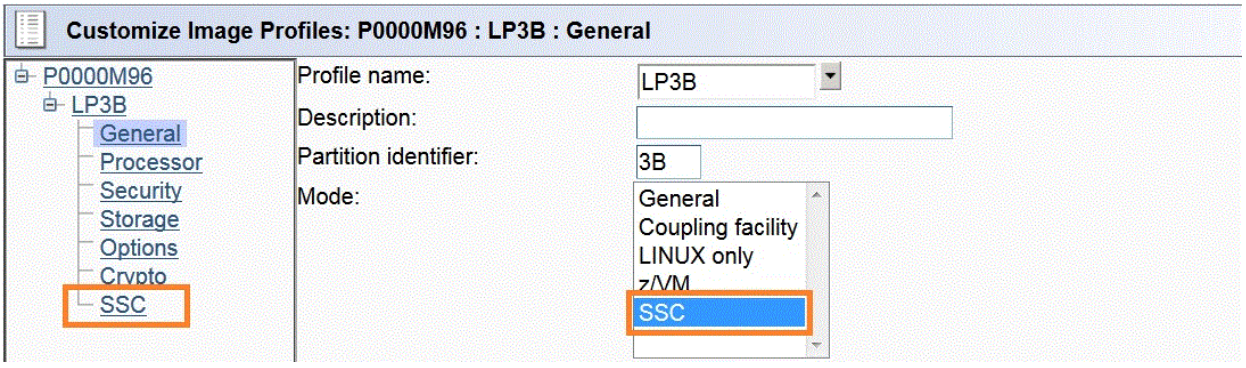

Figure 1. A portion of the General page of the Customize/Delete Activation Profiles task

- 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 on page 4 shows a sample screen capture of the **Create Partition** task 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.

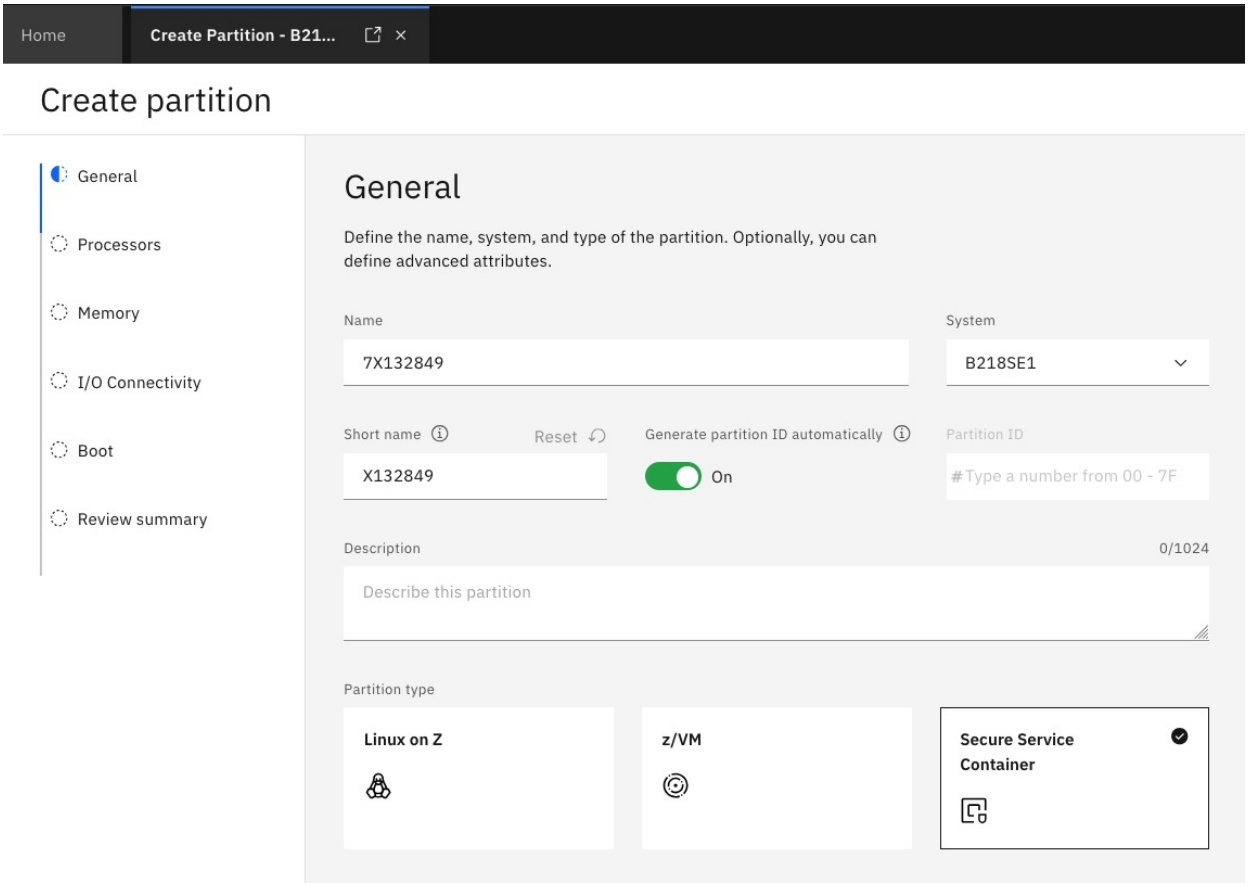

Figure 2. A portion of the General page of the Create Partition task

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.

Through this infrastructure, Secure Service Container provides:

- Quicker and simpler installation of 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 5.

Chapter 2. Prerequisites for using Secure Service Container

This topic provides information about the IBM Z and IBM LinuxONE (LinuxONE) systems that contain the IBM Secure Service Container.

You can configure Secure Service Container partitions on the following IBM Z and LinuxONE servers.

- IBM z17: machine type 9175
- IBM LinuxONE Rockhopper (Rockhopper V)
- IBM z16: machine types 3931 and 3932
- IBM z15: machine types 8561 and 8562
- IBM LinuxONE Next: machine type 9175
- IBM LinuxONE Emperor 4: machine type 3931
- IBM LinuxONE Rockhopper 4: machine type 3932
- IBM LinuxONE III: machine types 8561 and 8562

This topic describes the prerequisites for using the version of Secure Service Container that is available starting with the Hardware Management Console (HMC) / Support Element (SE) Version 2.15.0. For information about Secure Service Container for the previous version of the HMC/SE, see *Secure Service Container User's Guide*, SC28-6978.

The suggested practice is to use the latest available firmware for Secure Service Container, which is identified by the service bundle in Table 1 on page 5. To find the latest available service bundle, use the instructions for hardware updates in "Where to find hardware planning and corequisite software information" on page 9.

Table 1. Service bundles by machine type

Machine type	HMC/SE version and driver	Bundle
9175	Version 2.17.0 Driver 61	
3931 and 3932	Version 2.16.0 Driver 51	S04a or later
8561 and 8562	Version 2.15.0 Driver 41	S20b or later

Feature codes

Starting with IBM z16 (machine type 3931), hardware feature codes are no longer required for the use and support of appliances that run in a Secure Service Container partition. However, for systems prior to the IBM z16 (machine type 3931), you needed to order specific hardware feature codes to use the Linux® Hosting Foundation or Container Hosting Foundation offerings. For reference, those system machine types and hardware feature codes are documented in Appendix B, "Hardware feature codes," on page 71.

Upgrading to a new host system

Starting with IBM z16 (machine type 3931), the host system no longer supports appliances with wrapping key ID 0. Contact the appliance vendor to determine whether you can install a new or move an existing appliance to a Secure Service Container partition on an IBM z16.

Appliances have an associated wrapping key ID that indicates whether the appliance can be decrypted and started on a given host system. During the appliance installation process, the Secure Service Container installer displays the wrapping key ID when you select an appliance image to upload or select an existing disk to attach. Table 2 on page 6 lists the wrapping key ID values and indicates which host systems support them.

Table 2. Appliance wrapping key ID values that host systems support

Wrapping Key ID	IBM z17 host system	IBM z16 host system	z15 host system	z14 host systems
VERSION3.ROLL0	Supported	Not supported; the attempt to boot the appliance will fail	Not supported; the attempt to boot the appliance will fail	Not supported; the attempt to boot the appliance will fail
VERSION2.ROLL0	Supported	Supported	Not supported; the attempt to boot the appliance will fail	Not supported; the attempt to boot the appliance will fail
VERSION1.ROLL0	Supported	Supported	Supported	Not supported; the attempt to boot the appliance will fail
VERSION0.ROLL0	Supported	Supported	Supported	Supported

If the wrapping key is not supported by the host system on which the Secure Service Container partition resides, contact the appliance vendor for guidance.

How the host system mode affects your planning and installation tasks

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 DPM enabled, use the **Create Partition** task.

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 IBM Z or LinuxONE server 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.

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 HCD User's Guide*, SC34-2669, which is available in IBM Documentation at https://www.ibm.com/docs/en/zos/2.5.0?topic=zos-hcd
- *Input/Output Configuration Program User's Guide for ICP IOCP*, SB10-7177, which is available on **IBM Documentation**. Go to https://www.ibm.com/docs/en/systems-hardware, select **IBM Z** or **IBM LinuxONE**, then select your configuration, and click **Library Overview** on the navigation bar.

- For a host system with DPM enabled, DPM automatically detects the I/O adapters that are connected to the system. The DPM version determines which type of storage devices are available for use, and which method you use to configure them:
  - With DPM R3.0 or earlier, you can access FCP storage disks only. Use the HMC **Manage Adapters** task to manage the adapters for those storage devices.
  - With DPM R3.1 or later, you can access both FCP disks and FICON DASD. Use the **Configure Storage** task (instead of the **Manage Adapters** task) to configure storage adapters.
  - Starting with R4.3, DPM provides support for access to FCP tape storage through the **Configure Storage** task. However, although you can create and start a Secure Service Container partition that has tape links defined for access to FCP tape storage, Secure Service Container appliances do **not** support the use of tape storage devices.
  - Starting with R5.0, DPM introduces *partition links*, which interconnect two or more partitions that share the same network configuration and reside on the same system. With the introduction of partition links, DPM supports Version 2 of Shared Memory Communications - Direct Memory Access (SMC-D), which provides improved performance for communication between partitions on the same system. Use the **Configure Partition Links** to create, edit, or delete partition links, and to determine which partitions can use the partition links.
  - Starting with R5.2, DPM introduces two new types of partition links: FICON CTC and HiperSockets.

    FICON CTC partition links

    Fibre Connection (FICON) channel-to-channel (CTC) connections provide fast and efficient data transfer between systems, control units, and storage devices. Although FICON CTC technology supports interconnections between systems, a FICON CTC partition link can connect only partitions that reside on the same system. These partitions use the partition link only for data transfer among the group of partitions; a FICON CTC partition link does not provide access to storage devices.

    To create FICON CTC partition links, you can use the **Configure Partition Links** task on the HMC. To enable the Secure Service Container partition to use the partition link, add the Secure Service Container partition through the Partitions section of the **Configure Partition Links** task.

    HiperSockets partition links

    HiperSockets are virtual adapters that provide high-speed communications between partitions within a single system, without the need for any physical cabling or external networking connections. A HiperSockets partition link connects partitions that reside on the same system. To create HiperSockets partition links, you can use the **Configure Partition Links** task on the HMC.

    Support for HiperSockets is available in prior releases of DPM. When DPM R5.2 is installed on your system and the Support Element is restarted, any HiperSockets connections that were defined on a prior DPM release are automatically converted into HiperSockets partition links.

    - Any customized user permissions for existing HiperSockets adapters and tasks are not carried over from the prior configuration. In this case, your security administrator needs to set up equivalent user permissions for the new HiperSockets partition links.
    - If any Secure Service Container partitions use a HiperSockets connection to access the Secure Service Container web interface, you must reconfigure that connection to use an Open Systems Adapter-Express (OSA) adapter.

  For more information about prerequisites for using DPM, see the appropriate edition of the *IBM Dynamic Partition Manager Guide*, which is available on **IBM Documentation**. Go to https://www.ibm.com/docs/en/systems-hardware, select **IBM Z** or **IBM LinuxONE**, then select your configuration, and click **Library Overview** on the navigation bar.

Network and storage planning and prerequisites

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.

- Secure Service Container supports the use of Network Express adapters. Dynamic Partition Manager (DPM) supports the Network Express adapter only when it is configured in Hybrid mode. Network Express adapters configured as OSH/EQDIO are not supported.
- Starting with DPM R5.2, HiperSockets connections are no longer supported for accessing the Secure Service Container web interface on DPM-enabled host systems. To enable communication with the web interface, create a network interface card (NIC) that uses an Open Systems Adapter Express (OSA) adapter or Network Express adapter configured in hybrid mode. OSH is not supported.

  Note: The SSC Installer supports only OSA adapters with channel type OSD (Queued Direct I/O or QDIO mode). DPM host systems also support only the OSD channel type for OSA adapters. In contrast, standard host systems support additional channel types. When selecting an OSA adapter for use with an SSC partition, ensure that at least one adapter is configured with the OSD channel type.
- A Secure Service Container partition can use either port 0 or port 1 of an OSA adapter. Another SSC partition, or a different type of partition can use the remaining port on the same adapter.

  From a security perspective, a dedicated I/O resource is more secure than a shared one. If the appliance installed in the SSC partition requires a high level of security, consider configuring the OSA adapter as dedicated rather than shared
- Supported storage devices are Fibre Connection (FICON) Extended Count Key Data (ECKD) direct access storage devices (DASD) and Fibre Channel Protocol (FCP) disks.
- For FICON DASD:
  - Only channel subsystem (CSS) 0 and subchannel set ID (SSID) 0-2 are supported.
  - You can use parallel access volumes only when your storage administrator has activated the optional HyperPAV feature on the IBM System Storage DS8000® series, and has configured both base and alias volumes.
  - If you are installing to FICON DASD, avoid selecting a DASD size that is significantly larger than recommended size for the appliance (by hundreds of GB). Formatting a larger DASD can considerably slow down the installation.
- The target FCP disks and FICON DASD must be large enough to fit the uncompressed appliance. Check the recommended size for the appliance before proceeding with installation.

  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 worldwide 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**.

Appliances that can be installed in a Secure Service Container partition

Secure Service Container supports the following appliances.

- Linux container-based applications that are designed to run in Secure Service Container for IBM Cloud Private. For more information, see https://www.ibm.com/docs/en/sscfcp/1.1.0.3

- IBM Hyper Protect Virtual Servers, which protect Linux workloads on IBM Z and LinuxONE throughout the application lifecycle. For more information, see https://www.ibm.com/products/hyper-protect-virtual-servers
- IBM Hyper Protect Data Controller (formerly IBM Data Privacy Passports), through which you can encrypt your eligible data, grant and revoke access to it, and maintain control of it, even as it moves off the system of record within your enterprise. For more information, see https://www.ibm.com/products/hyper-protect-data-controller
- 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 Db2® Analytics Accelerator for z/OS®, which is a bundled solution package for the acceleration of database queries. It supports two deployment options, one of which requires a Secure Service Container; this deployment option is called the mainframe-only solution. For more information, see https://www.ibm.com/docs/en/daafz

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

Use the following links to find the most recent hardware planning and corequisite software information.

- 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.

Browser requirements and dependencies

The following tables list supported browser versions for the Secure Service Container installer and for using the user interface (UI) components for an installed appliance. The last table provides information about the Secure Service Container license file display.

The Secure Service Container (UI) requires the use of an HTML5-compliant web browser with JavaScript enabled. The latest version of the Secure Service Container allows only browsers with TLS 1.2 enabled.

Table 3. Supported browsers for the Secure Service Container installer

Browser	**Version**	**Operating system**
Firefox	82 and above	Windows, Linux
Chrome	101 and above	Windows, Linux

Table 4. Recommended, tested, and verified browsers for Secure Service Container appliances

Browser	**Version**	**Operating system**
Firefox	82 and above	Windows, Linux
Chrome	101 and above	Windows, Linux

Table 5. Secure Service Container license file display		
Browser	**Operating system**	**Display**
Firefox	Windows, Linux	The license file shown depends on the web page display language.
Chrome	Linux	The license file shown depends on the browser display language, which is controlled by the operating system locale.
Chrome	Windows	The license file shown depends on the browser display language, which can be set independently from the operating system console.

Multifactor Authentication

The Secure Service Container Installer uses username and password authentication only; multi-factor authentication (MFA) is not supported. If your security policies require MFA, you can implement network-based controls to restrict access to the Installer's IP address. For example, you can route access through a VPN configured to enforce MFA, an intermediate server, or another secure network path.

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

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 IBM Z 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

- Your installation must have correctly configured a supported host system and its I/O and storage devices. Check the list of prerequisites and information sources in Chapter 2, “Prerequisites for using Secure Service Container,” on page 5.
- 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 customized user ID with the predefined System Programmer Tasks role or equivalent permissions.

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.

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 embedded blanks. Valid characters for a profile name are:

      Characters 0 - 9
      Decimal digits

      Characters A - Z
      Letters of the English alphabet

      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.

4. Select the **Security** page and provide or modify any values 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 8192 MB (8 GB) of central storage is required to activate the Secure Service Container partition.

6. Select the **Options** page and provide or modify any values 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 3 on page 15 shows the **SSC** page elements.

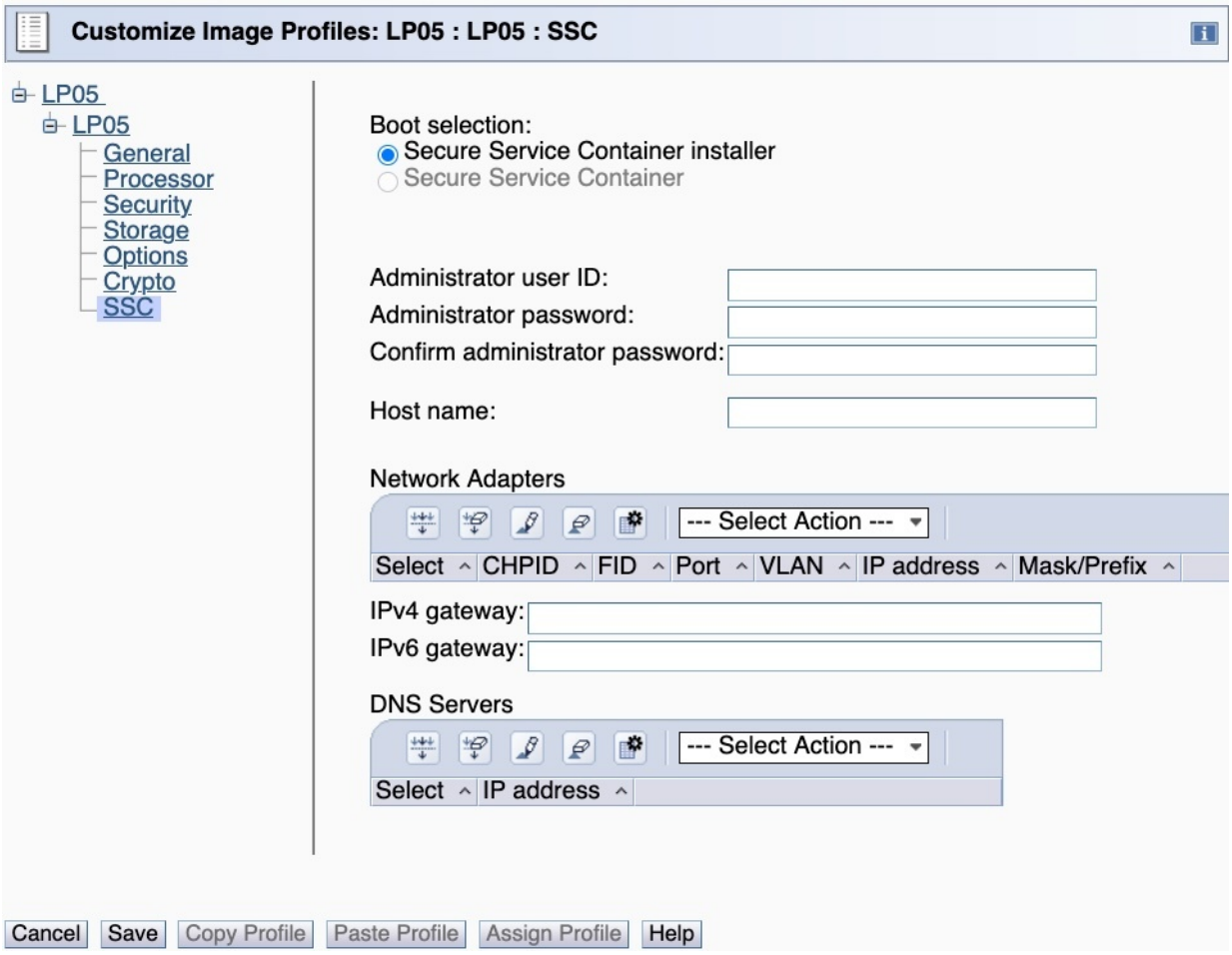

Figure 3. LPAR image profile: SSC page elements

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

b) Provide values for the default Administrator user ID and password.

Administrator user ID

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

Administrator 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 (-).

Administrator password

Enter the password for the administrator user ID. The administrator password can have a minimum of 8 characters and a maximum of 256 characters. The administrator 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 administrator password

Reenter the password exactly as you typed it for the Administrator 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 management network adapter configuration for the Secure Service Container (SSC) partition. This network connection is used by the SSC Installer GUI to manage the appliance installation and serves as the management entry point for the SSC appliance.

i) In the **Network Adapters** table, from the **Select Action** list, click **Add/Edit Network Adapters** to define a network connection. The **Add/Edit Network Adapters** window opens.

ii) For each type of network connection in the SSC environment, provide the required configuration details.

Note: Due to unpredictable behavior in the Address Resolution Protocol (ARP), it is recommended to assign only one network adapter per subnet. Using multiple adapters with IP addresses on the same subnet may result in delayed reachability, potentially up to 24 hours in large network environments.

FID
Enter the functional ID (FID) of the Network Express adapter.

CHPID

Enter the logical channel path identifier (CHPID) for the network adapter.

Note:

- For OSA adapters, ensure that three consecutive device IDs are configured in the I/O configuration for the CHPID.
- If you select an OSA adapter for use with an SSC partition, ensure that at least one adapter is configured with the OSD channel type. The SSC installer supports only OSA adapters with channel type OSD. Network Express adapter with channel type OSH is not supported.

PORT
It is valid for OSA adapters only. Select either port 0 or port 1. By default, port 0 is selected.

For network connections:

- You can assign the following IP address types to the same FID/VLAN or CHPID/VLAN set: DHCP IPv4, static IPv4, DHCP IPv6, and static IPv6.

  To do this, create one connection entry for IPv4 and another for IPv6.

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

i) Depending on the IP address type you selected for the network adapter, enter either an IPv4 address in the IPv4 gateway field, or an IPv6 address in the IPv6 gateway field. Do not include the mask or prefix for the gateway address.

ii) 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.

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

iv) 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 customized user ID that is assigned to one of the following predefined roles: System Programmer Tasks, Advanced Operator Tasks, or Operator Tasks.

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 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.
- 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.
- If you want to rename a Secure Service Container partition after you have already installed and run an appliance in it, complete the following steps:
  1. Use the **Deactivate** task to stop the partition.
  2. Through image page for the partition in the **Customize/Delete Activation Profiles** task:
     a. In the **General** section, edit the name of the partition.
     b. In the **SSC** section, make sure that the Boot selection is set to **Secure Service Container installer**.
     c. Save your changes.
  3. Use the **Activate** task to restart the partition. The Secure Service Container installer is restarted.
  4. To reboot the appliance successfully, follow the instructions in Chapter 15, “Moving an existing software appliance into a different Secure Service Container partition on the same system,” on page 63, making sure that you attach the existing disk that contains the 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 IBM Z 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 customized user ID with the predefined System Programmer Tasks role or equivalent permissions.

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 administrator 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 administrator user ID and password.

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

   Administrator 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 (-).

   Administrator password
   Enter the password for the administrator user ID. The administrator password can have a minimum of 8 characters and a maximum of 256 characters. The administrator 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 administrator password
   Reenter the password exactly as you typed it for the Administrator password field.
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, system programmers, or network administrators who are responsible for configuring logical partitions on IBM Z 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 customized user ID with the predefined System Programmer Tasks role or equivalent permissions.

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.

An administrator also can modify network settings from within an installed appliance, through the Secure Service Container UI network management component. For more information, see “Viewing and managing network connections” on page 52.

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) 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 (-).

   b) Customize the management network adapter configuration for the Secure Service Container (SSC) partition. This network connection is used by the SSC Installer GUI to manage the appliance installation and serves as the management entry point for the SSC appliance.

      i) In the **Network Adapters** table, from the **Select Action** list, click **Add/Edit Network Adapters** to define a network connection. The **Add/Edit Network Adapters** window opens.

      ii) For each type of network connection in the SSC environment, provide the required configuration details.

      Note: Due to unpredictable behavior in the Address Resolution Protocol (ARP), it is recommended to assign only one network adapter per subnet. Using multiple adapters with IP addresses on the same subnet may result in delayed reachability, potentially up to 24 hours in large network environments.

   FID
   Enter the functional ID (FID) of the Network Express adapter.

CHPID

Enter the logical channel path identifier (CHPID) for the network adapter.

Note: If you select an OSA adapter for use with a SSC partition, ensure that at least one adapter is configured with the OSD channel type. The SSC installer supports only OSA adapters with channel type OSD. Network Express adapter with channel type OSH is not supported.

PORT

It is valid for OSA adapters only. Select either port 0 or port 1. By default, port 0 is selected.

For network connections:

- You can assign the following IP address types to the same FID/VLAN or CHPID/VLAN set: DHCP IPv4, static IPv4, DHCP IPv6, and static IPv6.

  To do this, create one connection entry for IPv4 and another for IPv6.

c) Customize global network attributes for the Secure Service Container partition.

i) Depending on the IP address type you selected for the network adapter, enter either an IPv4 address in the IPv4 gateway field, or an IPv6 address in the IPv6 gateway field. Do not include the mask or prefix for the gateway address.

ii) 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.

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

iv) 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 customized user ID that is assigned to one of the following predefined roles: System Programmer Tasks, Advanced Operator Tasks, or Operator Tasks.

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 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 appliance 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 appliance.

   - 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.

Results

The image profile is either deleted or modified such that an appliance 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 DPM enabled. Topics include instructions for resetting login and network values.

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 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 IBM Z and LinuxONE servers. To configure a Secure Service Container partition on a DPM-enabled system, use the Hardware Management Console (HMC) **Create Partition** task to create a partition definition.

Before you begin

- Your installation must have correctly configured a supported host system and its I/O and storage devices. Check the topic Chapter 2, “Prerequisites for using Secure Service Container,” on page 5 for a list of requirements.
- Make sure you have the appropriate authorization to use the **Create Partition** task. You need to use either the predefined System Programmer Tasks role or a customized user role that is authorized to this task.
- Use the online help for the **Create 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 **Create Partition** task window.

About this task

The **Create 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 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 **Edit Partition** task, or use to start the partition through the **Start** task.

Procedure

1. Open the **Create Partition** task.

   You can access this task from the main HMC page by selecting the Systems Management node and expanding the Configuration task group, 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) Click the link for the **Create Partition** task.

      The **Create Partition** window opens, with an overlay that highlights key task controls on the window.

2. Required: Enter the name of the new partition, select the system, an optional short name, the partition type, and an optional description.

   The short name must uniquely identify the partition from all other partitions that are 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) Select the desired System from the drop down menu where you want the partition to be created.

c) To auto generate the partition ID, enable the option Generate partition ID automatically.

d) Optionally, specify a description for the partition. The description can be up to 1024 characters in length.

e) For partition type, select **Secure Service Container** from the list, as shown in Figure 4 on page 30.

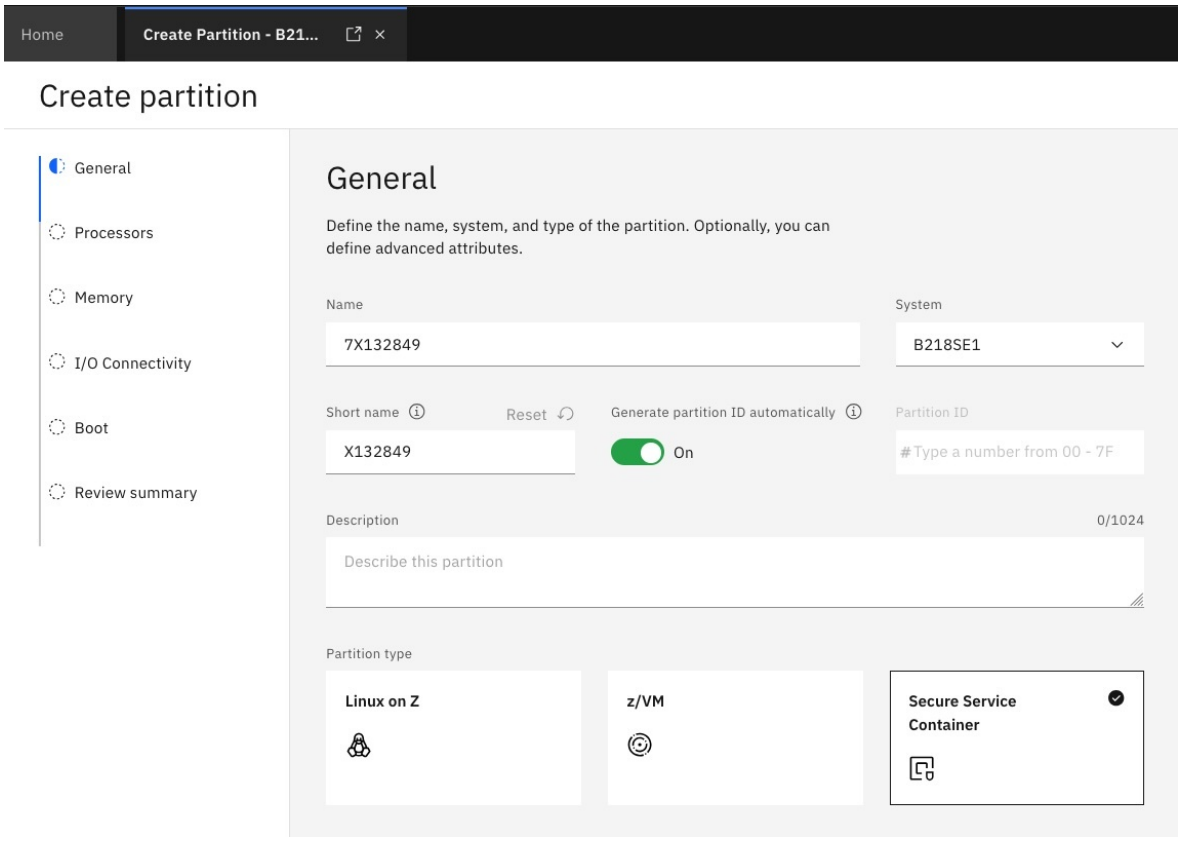

Figure 4. The General section of the Create Partition task

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

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

Administrator 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 (-).

Administrator password
Enter the password for the administrator user ID. The administrator password can have a minimum of 8 characters and a maximum of 256 characters. The administrator 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 administrator password
Reenter the password exactly as you typed it for the Administrator password field.

f) To reserve resources, select Yes. Otherwise, select No.

If you reserve resource, then your partition is guaranteed to be startable. Partitions without reserved resources might fail to start if sufficient resources are not available. The resources that are allocated will be unavailable for other partitions, even if the new partition is not active.

g) From the advance attributes, select the acceptable statuses and partition access controls.

Define the acceptable availability status values for the partition, based on the importance of its workload.

h) 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 shared virtual processors for the partition.

a) Select the processor mode.

In dedicate mode, the partition has dedicate physical processors. In shared mode, the partition shares the available physical processors with other partitions.

b) If the Processors type field is displayed, select a value. If you want to enable simultaneous multithreading for this partition, you must select the IFL processor type.

c) Select the number of processors that you want to assign to your new partition.

If you are creating a partition only to familiarize yourself with the process, you can accept the default value. Otherwise, base your selection on your knowledge of the processing requirements of the operating system and applications that you plan to run in this new partition.

d) Optional: Enable absolute processor capping limits the number of processors that the partition can use.

The partition cannot exceed this limit regardless of the availability of processors. You can enter the values in decimals to achieve fine-grained control over the resource allocation.

e) Optional: Set the processing weight value. Enforce weight capping, if needed.

The value assigned to processing weight is used to determine its relative share of processor time. A higher processor time means that the partition will receive more processing time.

f) Optional: Enable or disable the key import function that are available through CPACF Key Management Operation.

For operating systems and applications to take advantage of key encryption support, the partition in which they run must be configured to permit AES, DEA, ECC, and HMAC key import functions.

g) 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. If you are creating a partition only to familiarize yourself with the process, you can accept the default values for both the Memory and Maximum Memory fields. Otherwise, base your selection on your knowledge of the memory requirements of the operating system and applications that you plan to run in this new partition.

a) Review the Installed Memory bar chart to determine how much memory is available on this system, and how much is already in use or reserved for other partitions.

b) Select the amounts of initial and maximum memory that you want to assign to your new partition.

If you are creating a Secure Service Container partition, you must specify an initial amount of at least 4096 MB (4 GB). The minimum memory can increase up to the maximum memory setting when the partition is active.

c) To understand how your selection affects the availability of memory resources on the system, review the updated Installed Memory bar chart.

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

5. Required: Use the I/O Connectivity page to define 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 management NIC or a HiperSockets management NIC for communication.

To configure one or more NICs, follow these instructions.

a) Click **Network** and then click **Add adapter port**.

   Add adapters page lists the adapters that are available to the system.

b) Select the adapters and then click **Add adapter port**.

c) To modify the NIC's configurations, select the adapter, click **Options** and then click on **Configure NICs**.

   The **Configure NICs** page appears.

d) Enter a unique, meaningful name and, optionally, a description of the new NIC. and an optional description.

e) Enable **Use as management NIC**, the display includes the following configuration settings, which Secure Service Container partitions require for access to the web interface. For a Secure Service Container partition, you can select Network Express adapter in Hybrid mode, OSD adapter or HiperSockets adapter. Network Express adapter with channel type OSH is not supported.

   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. Note that DPM does not provide VLAN enforcement for Secure Service Container partitions.

   IP Address Type
   Select one of the following types:

   - **Static IPv4 Address**
   - **Static IPv6 Address**
   - **DHCPv4** (Dynamic Host Configuration Protocol)
   - **DHCPv6** (Dynamic Host Configuration Protocol)

   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.

f) Click **Configure NICs** to create the new NIC.

g) 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 as management NIC" switch to identify whether the NIC provides access to the web interface.

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

To configure Hipersocket management NIC, use the **Configure Partition Links** task

a) Launch **Configure Partition Links** task and provide name and the optional description.

b) Select the **system**, set the partition link type to `Hipersockets`, and then click **Next**.

c) Click **Add partitions**, and then add the SSC partition.

d) Navigate to the partition, I/O connectivity, and then Network

   You will see Hipersockets management NICs

e) Click **Add Management NIC**

f) Select the NIC and then click **Add Management NIC**

g) select the adapter, click **Options** and then click on **Configure interface**.

Provide the required details.

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. Note that DPM does not provide VLAN enforcement for Secure Service Container partitions.

IP Address Type
Select one of the following types:

- **Static IPv4 Address**
- **Static IPv6 Address**
- **DHCPv4** (Dynamic Host Configuration Protocol)
- **DHCPv6** (Dynamic Host Configuration Protocol)

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.

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

6. On the **Secure Service Container web interface communication** section, provide the required network settings that are displayed.

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. A default IPv4 gateway is required if you specified a Static IPv4 IP address type for the NIC.

Default IPv6 Gateway
Enter an IPv6 address for the default gateway. A default IPv6 gateway is required if you specified a Static IPv6 IP address type for the NIC.

DNS Server 1
Enter an IPv4 or IPv6 address for the primary domain name system (DNS) server.

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

7. To add a storage group or tape links, complete the following steps:

System administrators create storage groups and tape links to enable partitions (and the operating systems and applications that they host) to use physical storage hardware that is connected to the system. A *storage group* is a logical group of storage volumes that share certain attributes. A *tape link* defines the attributes of a connection that one or more partitions can use to access one FCP tape library in the SAN.

a) Click on Storage to attach storage groups .

Attaching a storage group or tape link enables the partition to access storage networks and hardware that is connected to the DPM-enabled system.

b) Click on Add storage group and then select the storage groups.

   Select one or more storage groups listed in the Storage Groups table to attach to this partition.

c) Click on tape links tab to add a tape link .

   Select one or more tape link to attach to this partition.

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. Use the information in the **Partition links** section to view or learn about partition links, which interconnect two or more partitions that share the same network configuration and reside on the same system.

   Through links in this section, you can open the **Configure Partition Links** task to the overview page, or open a new window to display the online help for that task.
10. On the Boot page, you can select the boot mode as either **Installer mode** or **Appliance mode**.

    When the partition starts, the system initializes the SSC Installer, allowing you to access the SSC web interface and install an appliance. You can choose to change the partition's boot mode from **Appliance Mode** to **Installer Mode**.
11. 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.
12. 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 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 customized user ID that is assigned to one of the following predefined roles: System Programmer Tasks, Advanced Operator Tasks, or Operator Tasks.

Procedure

1. Select the image for the Secure Service Container partition.
2. From the **Daily** task group, open the **Start** task.

   If the DPM R3.1 storage management feature or a later DPM version has been applied to the system, and one or more of the partitions to be started have attached storage groups that are being configured or modified, a warning message is displayed. The warning message includes the name of the affected partitions. The Start task does not continue until you make a selection.

   - Select **YES** to allow the affected partitions to be started.
   - Select **NO** to cancel the start operation for only the affected partitions.

   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 the DPM R3.1 storage management feature or a later DPM version has been applied to the system, the Details column contains messages that indicate the outcome. Otherwise, the Details column contains one of the following icons and labels, with a clickable **Details** link that identifies the failed partitions and provides a message that explains the failure.

   If the start operation 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.
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 boot mode in the Boot section of the **Partition Details** task.

Installed mode
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.

Appliance mode

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 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.

  To securely identify the partition to which your browser is connected, make a note of the fingerprint and the client key that are also displayed in the Operating System Messages. For example:

```
================================================================
Fingerprint of SSC Installer web certificate, use this to verify
your client connections.
----------------------------------------------------------------
Certificate:
subject=C = US, O = IBM, OU = zACI, CN = *.hostname
X509v3 Subject Alternative Name:
DNS:*.hostname, IP Address:192.0.2.0
SHA1 Fingerprint=4A:CE:4B:C6:C5:21:32:EC:39:D1:19:56:E2:3D:40:46:F3:CF:31:52
SHA256 Fingerprint=16:4E:E9:6A:7D:38:A0:C8:B2:65:98:85:66:AF:71:55:19:52:F8:FF:F
1:2F:61:85:2C:70:0E:07:8C:51:08:B6
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuhjx5iKYpWN0tz0jmNZd
4MSQZNGLZQtmcm4JzBpBn+Zv9nPC8N5b5wzgdwRXXeANwtk6BfVejj9C1AAMVRXT
GvrrziCw7ZrESqYhNsdoFE6LbrkaEIZyB2XuhbnrQN9n/YJwb8vQlV4RPM77ab/z
x765fNSIwAY+nCPJwACSuCORz5rg8zCc+xF/oWvMXMmaJ0EhXl+QaK6T56IA9NG8
owU0ubZXsTe6sf1VGE79M8DGr3T4C5/MVehCWa6InfK8dDJabgAG9pdzScBI0GrL
Bh0h19zHFQYaiwn/o7ZP6WFzQrC8FU541kwrlqVecNGO6x/qF6Qe3oQWBRo+CA9q
TwIDAQAB
-----END PUBLIC KEY-----
================================================================
```

- 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 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.
- If you add an active Secure Service Container partition to a FICON CTC, HiperSockets, or SMC-D partition link, you might need to use commands on the operating system to bring devices online so that partitions can use the partition link. For instructions and sample commands, see the online help for the **Configure Partition Links** task.
- If you want to rename a Secure Service Container partition after you have already installed and run an appliance in it, complete the following steps:

  1. Use the **Stop** task to stop the partition.
  2. Through the **Partition Details** task:
     a. In the **General** section, edit the short name of the partition.
     b. In the **Boot** section, make sure that the boot mode is set to **Installer Mode**.
     c. Save your changes.
  3. Use the **Start** task to restart the partition. The Secure Service Container installer is restarted.
  4. To reboot the appliance successfully, follow the instructions in Chapter 15, “Moving an existing software appliance into a different Secure Service Container partition on the same system,” on page 63, making sure that you attach the existing disk that contains the 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 IBM Z 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 customized user ID that is assigned to one of the following predefined roles: System Programmer Tasks, Advanced Operator Tasks, Operator Tasks, or Access Administrator Tasks.

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 administrator 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 and the click **Edit Partition**.
3. In the **General** section
   a) Replace the current values for either the default administrator user ID, the password, or both.

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

   Administrator 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 (-).

   Administrator password
   Enter the password for the administrator user ID. The administrator password can have a minimum of 8 characters and a maximum of 256 characters. The administrator 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 administrator password
   Reenter the password exactly as you typed it for the Administrator password field.
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.

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 IBM Z 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 customized user ID that is assigned to one of the following predefined roles: System Programmer Tasks, Advanced Operator Tasks, Operator Tasks, or Access Administrator Tasks.

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**.

An administrator also can modify network settings from within an installed appliance, through the Secure Service Container UI network management component. For more information, see “Viewing and managing network connections” on page 52.

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 and then click **Edit Partition.**
3. In the **Network** section,
   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. A default IPv4 gateway is required if you specified a Static IPv4 IP address type for the NIC.

   Default IPv6 Gateway
   Enter an IPv6 address for the default gateway. A default IPv6 gateway is required if you specified a Static IPv6 IP address type for the NIC.

   DNS Server 1
   Enter an IPv4 or IPv6 address for the primary domain name system (DNS) server.

   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.

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 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 customized user ID that is assigned to one of the following predefined roles: System Programmer Tasks, Advanced Operator Tasks, or Operator Tasks.

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 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 appliance 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.

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

   ii) 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.

   iii) 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.

   iv) 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.

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 appliance.
   - 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 appliance 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 appliance.

Part 4. Software appliances

This part contains step-by-step instructions for installing software appliances in a Secure Service Container partition, using the Secure Service Container user interface, and moving an existing appliance to another Secure Service Container partition.

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 5 to enable N Port Identifier Virtualization (NPIV).
- The target FCP disks and FICON DASD must be large enough to fit the uncompressed appliance. Check the recommended size for the appliance before proceeding with installation.
- 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. To securely identify the partition to which your browser is connected, make a note of the fingerprint and the client key that are also displayed in the Operating System Messages. For a sample display, see step “1” on page 46.
- You need to know the Administrator 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.
- Secure Service Container does not support multifactor authentication (MFA). However, you can enforce MFA using network-based rules to access Secure Service Container Installer IP address, if required by your security policies.
- 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 5.
- To avoid network latency, upload the appliance image from a browser on the same network as the Installer.
- If installing to FICON DASD, avoid selecting a DASD size that is hundreds of GB larger than the recommended size for the appliance, as formatting a large DASD can significantly slow down the installation.
- Slow I/O can affect installation time. If other workloads are consuming bandwidth on the storage server or channel subsystem, consider performing the installation when the system is less busy.

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.

   To verify your SSL connection, you can compare the fingerprint or public key information that your browser provides to the information that you find in the Operating System Messages display. For example:

   ```
   ====================================================================
   Fingerprint of SSC Installer web certificate, use this to verify
   your client connections.
   --------------------------------------------------------------------
   Certificate:
   subject=C = US, O = IBM, OU = zACI, CN = *.hostname
   X509v3 Subject Alternative Name:
   DNS:*.hostname, IP Address:192.0.2.0
   SHA1 Fingerprint=4A:CE:4B:C6:C5:21:32:EC:39:D1:19:56:E2:3D:40:46:F3:CF:31:52
   SHA256 Fingerprint=16:4E:E9:6A:7D:38:A0:C8:B2:65:98:85:66:AF:71:55:19:52:F8:FF:F
   1:2F:61:85:2C:70:0E:07:8C:51:08:B6
   -----BEGIN PUBLIC KEY-----
   MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuhjx5iKYpWN0tz0jmNZd
   4MSQZNGLZQtmcm4JzBpBn+Zv9nPC8N5b5wzgdwRXXeANwtk6BfVejj9C1AAMVRXT
   GvrrziCw7ZrESqYhNsdoFE6LbrkaEIZyB2XuhbnrQN9n/YJwb8vQlV4RPM77ab/z
   x765fNSIwAY+nCPJwACSuCORz5rg8zCc+xF/oWvMXMmaJ0EhXl+QaK6T56IA9NG8
   owU0ubZXsTe6sf1VGE79M8DGr3T4C5/MVehCWa6InfK8dDJabgAG9pdzScBI0GrL
   Bh0h19zHFQYaiwn/o7ZP6WFzQrC8FU541kwrlqVecNGO6x/qF6Qe3oQWBRo+CA9q
   TwIDAQAB
   -----END PUBLIC KEY-----
   ====================================================================
   ```

2. On the Login page, enter the Administrator 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) In the **Image Details** section, check the value that is listed for Wrapping Key ID to determine whether the appliance can be decrypted and started on the host system.

   Figure 5 on page 47 shows a sample screen in which the Wrapping Key ID field is highlighted.

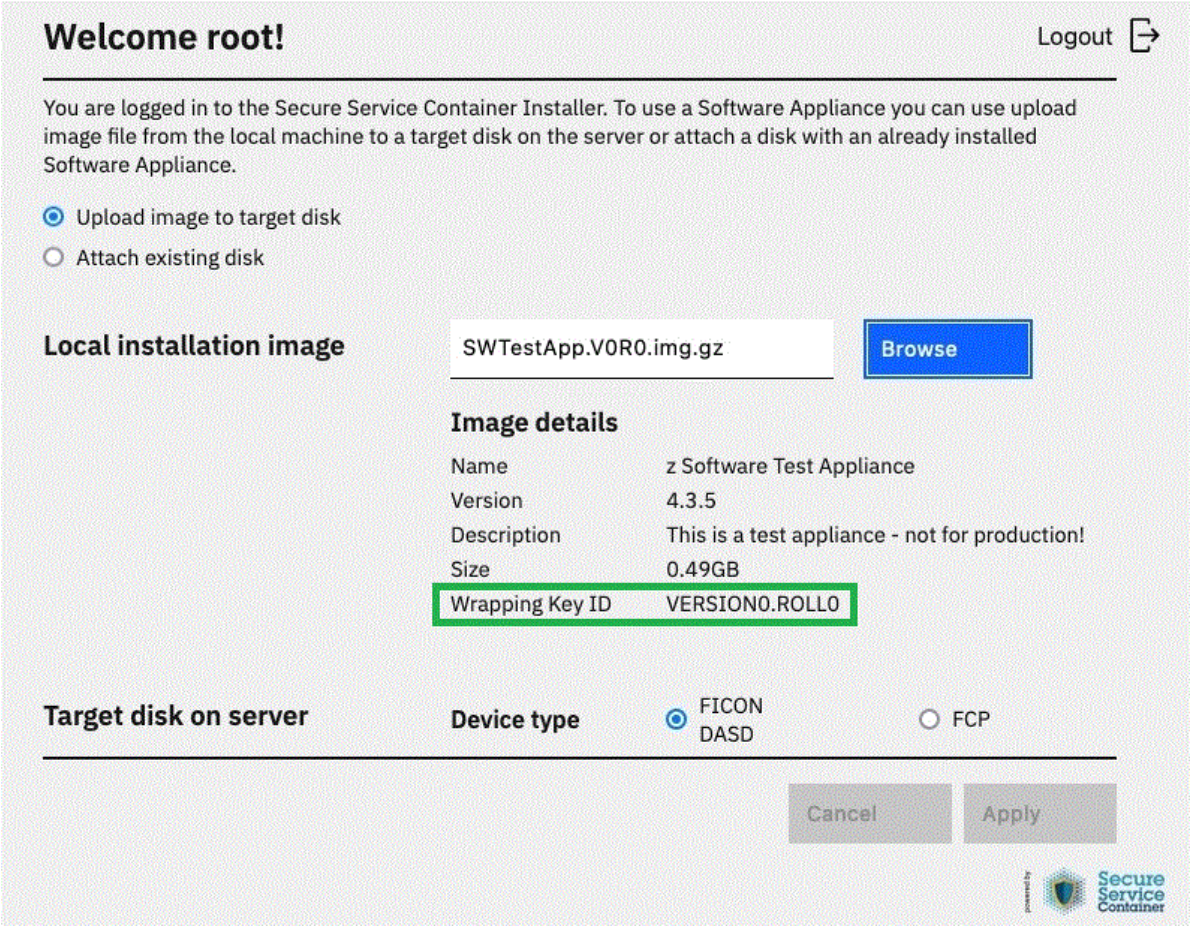

Figure 5. Sample screen displaying the wrapping key ID of an appliance

The wrapping key ID indicates whether the appliance can be decrypted and started. If the wrapping key is not supported by the host system on which the Secure Service Container partition resides, the appliance cannot start. Table 6 on page 47 lists the wrapping key ID values and indicates which host systems support them.

Table 6. Appliance wrapping key ID values that host systems support

Wrapping Key ID	IBM z17 host system	IBM z16 host system	z15 host system	z14 host systems
VERSION3.ROLL0	Supported	Not supported; the attempt to boot the appliance will fail	Not supported; the attempt to boot the appliance will fail	Not supported; the attempt to boot the appliance will fail
VERSION2.ROLL0	Supported	Supported	Not supported; the attempt to boot the appliance will fail	Not supported; the attempt to boot the appliance will fail
VERSION1.ROLL0	Supported	Supported	Supported	Not supported; the attempt to boot the appliance will fail
VERSION0.ROLL0	Supported	Supported	Supported	Supported

- If the wrapping key ID is not supported on the system that hosts the Secure Service Container partition, do not continue this procedure. Use information from the appliance provider to upgrade the appliance.
- If the wrapping key ID is supported on the host system, continue to step "4.d" on page 48.

d) 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.

Note: For FICON DASD, only channel subsystem (CSS) 0 and subchannel set ID (SSID) 0-2 are supported. Also, make sure that you specify a four-character hexadecimal device number.

FCP

If you select **FCP** as the device type, select one of the options that are 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. Both the WWPN and LUN must be 16-character hexadecimal numbers.

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.

e) 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 restart.

a. When the restart process begins, the installer displays the restart 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, if that is page is provided by the appliance.

6. If available, on the appliance page, complete the following steps.

a) If prompted by your browser, accept the self-signed certificate for the SSL connection.

To verify your SSL connection, you can compare the fingerprint or public key information that your browser provides to the information that you find in the Operating System Messages display. For example:

```
Certificate '192.0.2.0:4431:
subject=C = US, 0 = IBM, OU = ZACI, CN = * .hostname
X509v3 Subject Alternative Name:
DNS:*.hostname, IP Address:192.0.2.0
SHA1 Fingerprint=B5:1D:05:65:8C:E8:15:B8:17:06:14:1A:B9:2A: FB: 4E:61:7B:09:E0
- - - - -BEGIN PUBLIC KEY- - - - -
MIIBIJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA62JjRpF2cInQFcqHkXqb
INsyUIpDYoymv8FkFLrFdaG7aQpyjdl+JSasRSsfFVopi/sAOzhUfOiWCAaS8/SO
6fkebTVE5GSZObqF35Cttn79h6EKxhTutqxUV5hJ8eKS96ixoaYhw/LRG+eZ/HSf
JET5due7492VYMOeYUW03YOSZnzM7hMag93APAjpPomppArtgJeCJYOap20mtEwa
```

```
RIqdSi2zxe+yKd433CIgitJB5Ffq8oxm25eB1riw22fZ/GiFKbddmivnRa3rXSz2
zsOieywHwi8qk7BQbMh77tBX6mFRovrrk0h42+VLFjkpOTINm494tUPaibXy920K
nWIDAQAB
- - - - -END PUBLIC KEY- - - - -
```

b) Enter the administrator 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.

If a problem occurs, the installer displays an error message that can help you troubleshoot problems that are related to user input. If the message indicates an internal problem, see Appendix A, “Codes from the Secure Service Container installer,” on page 69.

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

The topic provides an overview of the Secure Service Container user interface (UI) components.

Note: Appliances that are designed to run in a Secure Service Container (SSC) partition can use one or more SSC user interface (UI) components. These components allow you to view partition network and login settings, request a partition data dump for problem reporting to IBM, and perform additional management tasks.

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

- 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 Administrator 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 components that are displayed in the navigation bar. Figure 6 on page 51 shows a partial screen display with the component icons in the navigation frame. For information about browser requirements, see “Browser requirements and dependencies” on page 9.

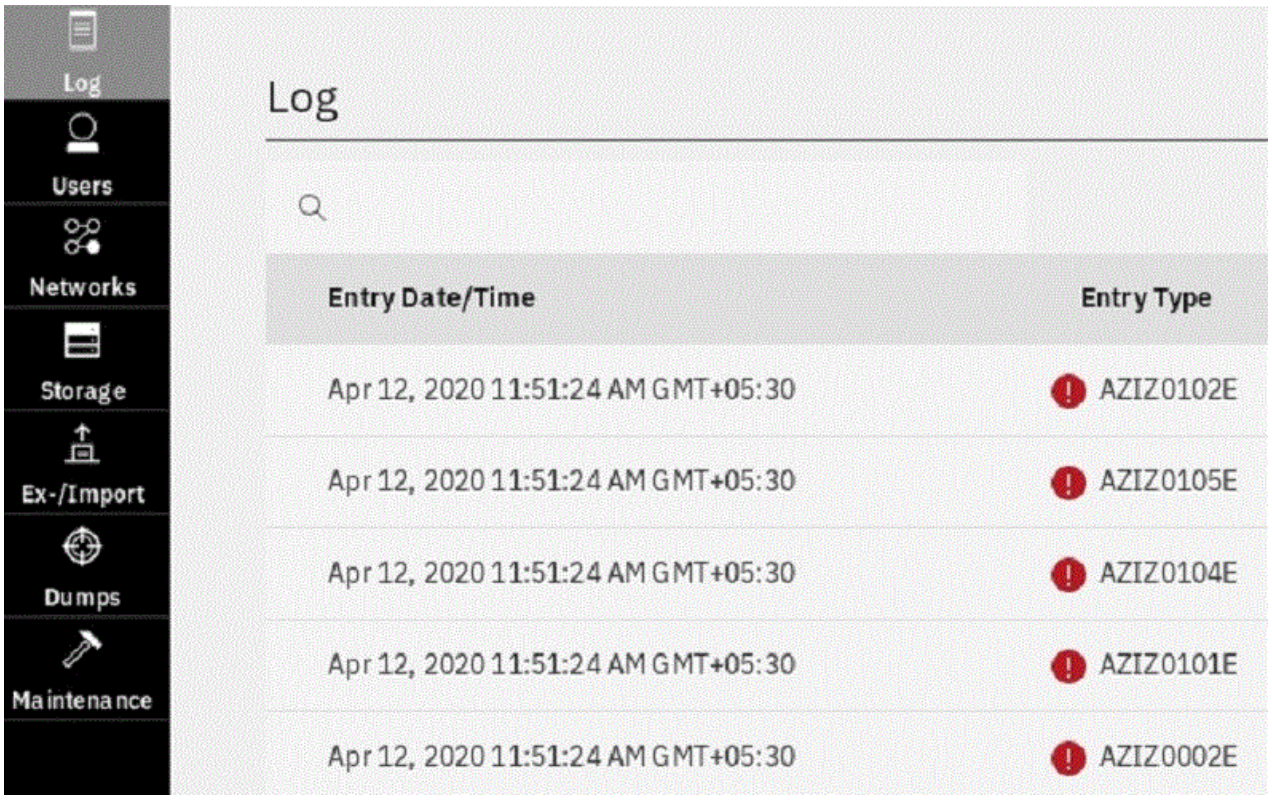

Figure 6. Sample screen with UI component icons in the navigation frame

1. The **Log** component 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** component.

2. The **Users** component provides functions through which you can manage users, roles, and groups, as well as authentication and authorization. Specifically, you can complete the following tasks.
   - List and view details about users, roles, and groups.
   - Add, modify, or remove users and groups.
   - Initiate (or raise) a request to reset the password for one or more users.
   - View a list of the requests to reset passwords.
   - Generate and retrieve a reset password link to fulfill a request to reset a password.
3. The **Networks** component displays the status and details for the network interfaces that are defined for the Secure Service Container partition and the installed appliance. The Networks component also includes controls through which you can manage network connections for the appliance. For more information, see "Viewing and managing network connections" on page 52.
4. The **Storage** component displays the status and details of attached storage devices. The Storage component also includes controls through which you can modify a storage pool by adding either FICON DASD or FCP disks.

   Before you can use the **Storage** component, an administrator must add storage resources to the Secure Service Container partition. The host-system mode determines how storage resources are configured, as described in Chapter 2, "Prerequisites for using Secure Service Container," on page 5.

   For more information about the **Storage** component, see "Viewing and managing storage resources" on page 55.
5. The **Ex-/Import** component provides controls through which users can export or import appliance data. For more information, see "Exporting or importing appliance configuration data" on page 60.
6. The **Dumps** component 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 61.
7. The **Maintenance** component provides a way to shut down a currently running appliance and automatically reboot the Secure Service Container installer in the partition. Use this function to upgrade an existing or install a new appliance. For more information, see "Rebooting the Secure Service Container installer" on page 61.

Viewing and managing network connections

Through the Networks user interface (UI) component, you can view and manage the network connections for an appliance that is installed in a Secure Service Container partition. The alternative method is to use the appropriate HMC task on the system on which the Secure Service Container resides: the **Customize/Delete Activation Profile** task on a standard mode system, or the **Partition Details** task on a DPM-enabled system.

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 the following information.

- 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. However, if an administrator overwrote the HMC network settings through the UI **Networks** component for the installed appliance, you need to specify the IP address of the network adapter as specified in the UI component.

- You need to know the Administrator 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.

About this task

You can use the **Networks** component in the Secure Service Container UI to either view or manage network connections for the appliance. Initially, the list of network connections reflects the network information that an administrator specified when defining the partition through the HMC. The list view includes the following details for each type of network connection: name, status, type (Ethernet or VLAN), device number, and IPv4 or IPv6 addresses. You can filter the list or modify its contents through icons at the top of the **Network Connections** page.

Through the **Networks** component, you can add, activate, deactivate, or remove the following types of network connections.

- Ethernet-type connections through which the appliance can communicate over IBM HiperSockets or Open Systems Adapter-Express (OSA-Express) devices.
- VLAN-type connections that associate a VLAN ID with a parent device (that is, an Ethernet-type connection).
- Bond-type connections that combine multiple network interfaces of the same kind (for example, two eth0 interfaces) into a single virtual link.

Important:

- When you modify network connections through the **Networks** component, these changes are **not** reflected in the HMC image profile or partition definition for the Secure Service Container partition.
- Although you can dynamically add, remove, or change network adapters for an active LPAR or partition through either HCD or the HMC on a standard (PR/SM) system, or through the HMC on a DPM-enabled system, these dynamic changes do not affect a running Secure Service Container appliance. For those dynamic configuration changes to take effect:
  - On a standard system, you must deactivate and reactivate the LPAR.
  - On a DPM-enabled system, you must stop and restart the partition.

Procedure

1. In the navigation pane, click the **Network** icon to display the **Network Connections** page.

   The **Network Connections** page opens.
2. To add a new connection, click the plus (+) icon on the top right of the page, and select **Ethernet** or **VLAN** or **Bond**.

   Depending on the connection type that you selected, one of the following pages opens.

   - **Add Ethernet Connection**: for instructions, go to step “3” on page 53.
   - **Add VLAN Connection**: for instructions, go to step “4” on page 54.
   - **Add Bond**: for instructions, go to step “5” on page 54.
3. If you are adding an Ethernet connection, complete the following steps.
   a) On the **General** tab, select a network device from the list of unconfigured devices.

      The Device Details section displays information about the network device, and the Connection Name field is automatically populated with a name that you can edit.

   b) Choose a connection state: **Active** automatically activates the connection after it is created, and **Inactive** stores the connection properties for later use.

   c) Optional: Select the **IPv4** tab or the **IPv6** tab to complete the network connection configuration. You can specify both IPv4 and IPv6 addresses for the same network connection. If you do not provide any information on one of these tabs, the network connection is defined with Dynamic Host Configuration Protocol (DHCP) address mode.

i) Select one of the following address modes.

Manual
Select this mode to enter specific address settings: address, prefix, and gateway. You can specify only a single gateway, but multiple IP addresses (with their corresponding prefixes) per connection.

Automatic
Select this mode to use a DHCP address.

Disabled
Select this mode to define the network connection without configuring an address.

d) Click **Add** to add the connection and return to the **Network Connections** page.

4. If you are adding a VLAN connection, complete the following steps.

a) On the **General** tab, select a parent device from the list of unconfigured devices or click the plus (+) icon to create a new parent device.

If you click the plus icon, complete the following steps; otherwise, continue to step "4.b" on page 54.

i) On the **Create New Parent Device for VLAN** page, select a network device from the list of unconfigured devices. The Device Details section displays information about the network device.

ii) If the network device supports multiple ports, select port **0** or **1** in the Port list.

iii) Click **Create** to create the device and return to the **General** tab.

b) Select a VLAN ID and choose a connection state: **Active** automatically activates the connection after it is created, and **Inactive** stores the connection properties for later use.

c) Optional: Select the **IPv4** tab or the **IPv6** tab to complete the network connection configuration. You can specify both IPv4 and IPv6 addresses for the same network connection. If you do not provide any information on one of these tabs, the network connection is defined with Dynamic Host Configuration Protocol (DHCP) address mode.

i) Select one of the following address modes.

Manual
Select this mode to enter specific address settings: address, prefix, and gateway. You can specify only a single gateway, but multiple IP addresses (with their corresponding prefixes) per connection.

Automatic
Select this mode to use a DHCP address.

Disabled
Select this mode to define the network connection without configuring an address.

d) Click **Add** to add the VLAN connection and return to the **Network Connections** page.

5. If you are adding a Bond connection, complete the following steps.

a) On the **General** tab, fill in or select values for the required fields.

- Provide a connection name to uniquely identify the connection, and a bond device ID.
- Add one or more slave connections by selecting the plus (+) icon. For each slave, select a network device and port number, then click **Yes** to add the device.
- Select a mode for the bond network connection. If you want to specify values for advanced options, click the circled arrow icon to the right of the **Mode** field to view the list of options.
- Select values for link monitoring and delay options, and the connection state.

b) Optional: Select the **IPv4** tab or the **IPv6** tab to complete the network connection configuration. You can specify both IPv4 and IPv6 addresses for the same network connection. If you do not provide any information on one of these tabs, the network connection is defined with Dynamic Host Configuration Protocol (DHCP) address mode.

i) Select one of the following address modes.

Manual
Select this mode to enter specific address settings: address, prefix, and gateway. You can specify only a single gateway, but multiple IP addresses (with their corresponding prefixes) per connection.

Automatic
Select this mode to use a DHCP address.

Disabled
Select this mode to define the network connection without configuring an address.

c) Click **Add** to add the Bond connection and return to the **Network Connections** page.

Results

Depending on the address mode that you selected, network connections that you defined for the appliance are either saved and activated, or saved for later use.

What to do next

You can use the icon controls on the top right of the **Network Connections** page to manage the newly defined network connections.

To modify a network connection

1. Select a network connection listed in the table on the **Network Connections** page.
2. Either double-click the table entry or click **Edit** (pencil icon) to modify details about the network connection. For both Ethernet or VLAN connections, you can modify any properties on the **General**, **IPv4**, or **IPv6** pages; however, you cannot change the network device. For Bond connections, you can modify any properties on the **General**, **IPv4**, or **IPv6** pages; however, you cannot modify the bond device ID.
3. Click **Update** to save the modified properties.

To activate a network connection

1. Select an inactive network connection listed in the table on the **Network Connections** page. Use the Status indicator to determine which network connections are active (green) or inactive (orange).
2. Click **Activate** (icon of a triangle pointing to the right) to enable all of the configuration properties for the selected network connection, so it can be used for communication.
3. In the confirmation dialog, click **Yes** to continue the operation, or **No** to cancel it.

To deactivate a network connection

1. Select an active network connection listed in the table on the **Network Connections** page. Use the Status indicator to determine which network connections are active (green) or inactive (orange).
2. Click **Stop** (icon of a square) to deactivate the selected network connection.
3. In the confirmation dialog, click **Yes** to continue the operation, or **No** to cancel it.

To remove a network connection

1. Select a network connection listed in the table on the **Network Connections** page.
2. Click **Remove** (trash can icon) to remove the selected network connection.
3. In the confirmation dialog, click **Yes** to continue the operation, or **No** to cancel it.

Viewing and managing storage resources

Through the Storage user interface (UI) component, you can view and manage the storage resources for an appliance that is installed in a Secure Service Container partition. Storage resources are grouped into storage pools that are created when the appliance is built. A *storage pool* is a uniquely named collection of storage disks on which the appliance file system is mounted.

Supported storage devices are Fibre Connection (FICON) Extended Count Key Data (ECKD) direct access storage devices (DASD), and Fibre Channel Protocol (FCP) disks. Each storage pool must contain only one type of storage: either FICON DASD or FCP disks. The host-system mode determines which types of storage resources you can use.

- For a host system running in standard mode (that is, with Processor Resource/System Manager or PR/SM), supported storage devices are FICON DASD and FCP disks. For FICON DASD, only channel subsystem (CSS) 0 and subchannel set ID (SSID) 0-2 are supported.
- For a host system with DPM enabled, the DPM version determines the supported storage types.
  - With DPM R3.0 or earlier, you can access FCP storage disks only.
  - With DPM R3.1 or later, you can access both FCP disks and FICON DASD.
  - Starting with R4.3, DPM provides support for access to FCP tape storage. However, although you can create and start a Secure Service Container partition that has tape links defined for access to FCP tape storage, Secure Service Container appliances do **not** support the use of tape storage devices.

From the Secure Service Container user interface (UI), you can view the storage pools for an installed appliance by selecting the **Storage** icon in the navigation pane. This action opens the **Storage Disks by Storage Pool** page, which contains a table-like display with alternating rows, as shown in Figure 7 on page 56. You can filter the display by typing the storage pool name in the Filter field, or selecting the name from the **All Storage Pools** list.

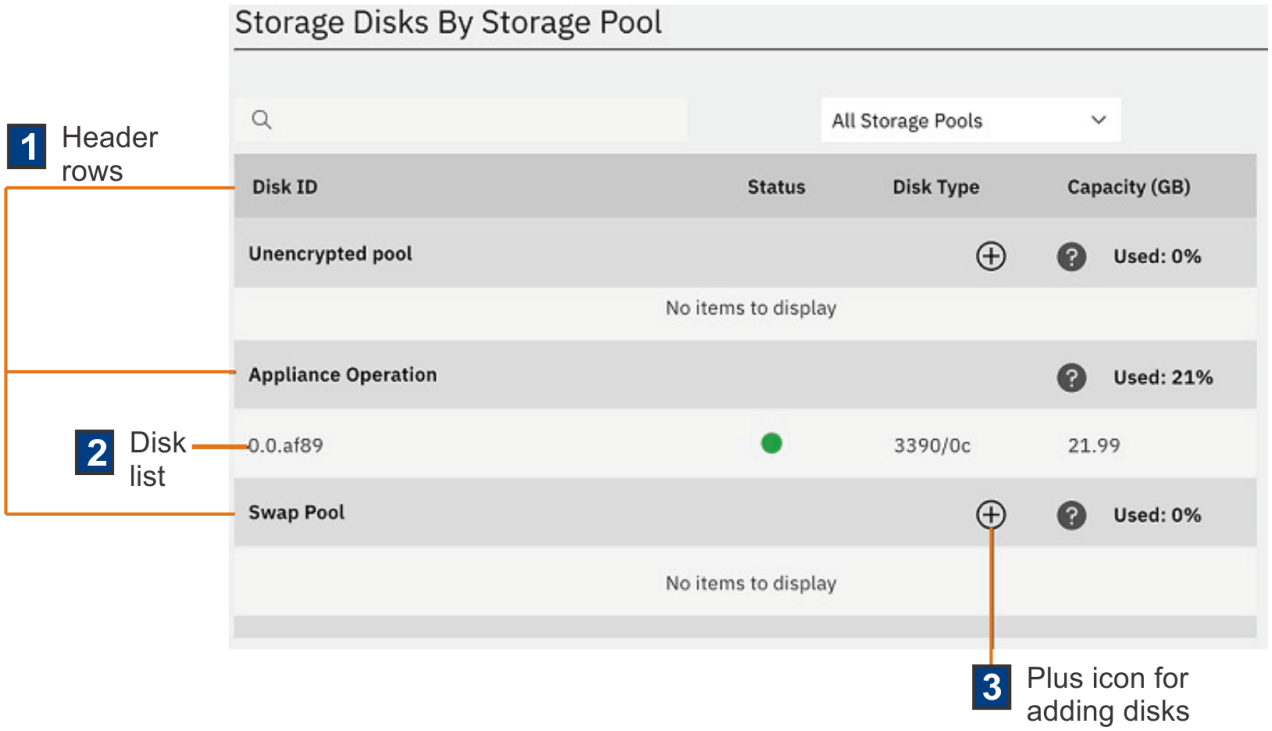

*Figure 7. Sample display of the **Storage Disks by Storage Pool** page*

The list of storage pools on the **Storage Disks by Storage Pool** page contains the following elements.

1. A highlighted header row for each defined storage pool for the installed appliance. For each storage pool, the header row contains the following information or controls.
   - The storage pool name.
   - The plus (+) icon that you can select to add disks to the storage pool. Note that this control is not available for the Appliance Operation storage pool, which cannot be modified.
   - The hint (?) icon that you can select to display the properties of the storage pool.
   - The percentage of the total disk capacity that is in use.

2. One or more rows that list details about the disks in the storage pool. Each row contains the following information.

   Disk ID
   Specifies the disk identifier, which varies, depending on the type of storage disk.

   - For an FCP disk, the ID is the universally unique identifier (UUID) of the volume.
   - For FICON DASD, the ID is a combination of the logical control unit (LCU) number and volume ID.

   Status
   Indicates that the disk is available (green dot) or not available (red dot).

   Disk Type
   Specifies whether the disk is FICON DASD or an FCP disk.

   Capacity
   Indicates the disk capacity in gigabytes (GB).

To add disks to a storage pool, see the appropriate topic.

- "Adding FICON DASD to available storage pools" on page 57
- "Adding FCP disks to available storage pools" on page 58

If the Storage UI component is not implemented for the installed appliance, the alternative method of viewing and managing storage is to use the appropriate HMC view or task on the system on which the Secure Service Container partition resides. The host-system mode determines which HMC view or task to use.

- 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**.
- For a host system with DPM enabled, the DPM version determines where storage details are specified. With DPM R3.0 or earlier, storage details are specified in the IOCDS that is in effect for the host system. With DPM R3.1 or later, storage details are specified on the Storage Overview page of the HMC **Configure Storage** task. To view or modify storage information for the Secure Service Container partition, use the **Partition Details** task.

Important: Although you can dynamically add, remove, or change storage adapters for an active LPAR or partition through either HCD or the HMC on a standard (PR/SM) system, or through the HMC on a DPM-enabled system, these dynamic changes do not affect a running Secure Service Container appliance. For those dynamic configuration changes to take effect:

- On a standard system, you must deactivate and reactivate the LPAR.
- On a DPM-enabled system, you must stop and restart the partition.

Adding FICON DASD to available storage pools

Use these instructions to add FICON DASD to an existing storage pool for an appliance. You can add not only base volumes but also alias volumes, only when your storage administrator has activated the optional HyperPAV feature on the IBM System Storage DS8000 series, and has configured both base and alias volumes. In this case, you must add the base volumes to a storage pool *before* adding alias volumes to the same pool.

Before you begin

Attention: When you add disks to a storage pool, any existing data that is on those disks is lost when the disks are formatted.

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 the following information.

- 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. However, if an administrator overwrote the HMC network settings through the UI **Networks** component for the installed appliance, you need to specify the IP address of the network adapter as specified in the UI component.
- You need to know the Administrator 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. Log in to the Secure Service Container user interface (UI).
2. In the navigation pane, click the **Storage** icon to display the **Storage Disks by Storage Pool** page.
3. To add FICON DASD to a storage pool, select the plus (+) icon in the header row for the storage pool.

   By default, the **Add Storage Disks to Storage Pool** page opens with the **FICON DASD** tab selected.
4. In the **Available Devices** list, review the devices that you can add to the storage pool.

   The counter under the **Available Devices** list indicates how many devices are available. If necessary, you can scroll through the list, select how many entries to display at one time, or filter the list by typing in the Filter field.

   a) Select either Assign (**>**) to add only selected devices, or Assign All (**>>**) to add any available devices that match the filter that you set. If you did not set a filter, Assign All adds all available devices to the storage pool.

      The devices are moved from the **Available Devices** list to the **Assigned to Pool** list.

   b) Select **Apply** to assign the devices to the storage pool.
5. On the **Confirm Add Disk** page, review the disks to be added and select **Yes** to continue the operation.

   The FICON DASD are added to the storage pool asynchronously. On the **Storage Disks by Storage Pool** page, the Status column entry displays a progress indicator and message that indicates which step of the operation is underway. You cannot add any more disks until all steps of the operation have been completed.

Results

When the Status column entry changes from the progress indicator to a green dot, the FICON DASD are ready for use in the storage pool.

What to do next

If you want to add HyperPAV alias volumes to the same storage pool, repeat the steps in this procedure, adding the alias devices that are assigned to the base volumes. Note that you must successfully add the base volumes to the storage group *before* you can add the alias volumes.

Adding FCP disks to available storage pools

Use these instructions to add FCP disks to an existing storage pool for an appliance.

Before you begin

Attention: When you add disks to a storage pool, any existing data that is on those disks is lost when the disks are formatted.

- 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 the following information.
  - 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. However, if

an administrator overwrote the HMC network settings through the UI **Networks** component for the installed appliance, you need to specify the IP address of the network adapter as specified in the UI component.

  - You need to know the Administrator 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.

- To enable Secure Service Container to discover FCP disks that you can add to a storage pool, make sure that your installation has completed the required steps in Chapter 2, "Prerequisites for using Secure Service Container," on page 5 to enable N Port Identifier Virtualization (NPIV).

Procedure

1. Log in to the Secure Service Container user interface (UI).
2. In the navigation pane, click the **Storage** icon to display the **Storage Disks by Storage Pool** page.
3. To add FCP disks to a storage pool, select the plus (+) icon in the header row for the storage pool.

   By default, the **Add Storage Disks to Storage Pool** page opens with the **FICON DASD** tab selected.
4. Select the **FCP** tab to display the controls for discovering and adding FCP disks to the storage pool.
   a) Select one of the following discovery methods: **Scan all devices**, **Scan single device only**, or **Manual**.

      Scan all devices
      Scans all FCP adapters for which NPIV is enabled.

      Scan single device only
      Scans only one FCP adapter for which NPIV is enabled. Select the FCP adapter from the **Device** list.

      Manual
      Scans only the FCP device for which you provide the FCP path information.

      i) Select the FCP adapter from the **Device** list.

      ii) In the Target WWPN field, provide the 16-character hexadecimal worldwide port number (WWPN) of the storage controller.

      iii) In the LUN field, provide the 16-character hexadecimal logical unit (LUN) identifier.

   b) Select **Discover** to start the discovery operation. If you selected **Scan all devices**, the **Discovered Volumes** pane displays a progress indicator. In this case, the discovery operation can take some time, depending on the number of configured adapters, and the number of disks that are assigned to each adapter.

      When the operation completes, available disk volumes are listed in the **Discovered Volumes** pane.
5. In the **Discovered Volumes** list, review the disk volumes that you can add to the storage pool.

   The counter under the **Discovered Volumes** list indicates how many volumes are available. If necessary, you can scroll through the list, select how many entries to display at one time, or filter the list by typing in the Filter field.

   a) Select either Assign (**>**) to add only selected volumes, or Assign All (**>>**) to add any available volumes that match the filter that you set. If you did not set a filter, Assign All adds all available volumes to the storage pool.

      The volumes are moved from the **Discovered Volumes** list to the **Assigned to Pool** list.

   b) Select **Apply** to assign the volumes to the storage pool.
6. On the **Confirm Add Disk** page, review the disk volumes to be added and select **Yes** to continue the operation.

   The disk volumes are added to the storage pool asynchronously. On the **Storage Disks by Storage Pool** page, the Status column entry displays a progress indicator and message that indicates which step of the operation is underway. You cannot add any more disks until all steps of the operation have been completed.

Results

When the Status column entry changes from the progress indicator to a green dot, the FCP disk volumes are ready for use in the storage pool.

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 component.

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. However, if an administrator overwrote the HMC network settings through the UI **Networks** component for the installed appliance, you need to specify the IP address of the network adapter as specified in the UI component.
- You need to know the Administrator 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**.

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 component.

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. However, if an administrator overwrote the HMC network settings through the UI **Networks** component for the installed appliance, you need to specify the IP address of the network adapter as specified in the UI component.
- You need to know the Administrator 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 (a plus sign) 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.

Rebooting the Secure Service Container installer

Through the Maintenance user interface (UI) component, you can shut down a currently running appliance and automatically reboot the Secure Service Container installer in the partition. The alternative method

is to use the appropriate HMC task on the system on which the Secure Service Container resides: the **Customize/Delete Activation Profile** task on a standard mode system, or the **Partition Details** task on a DPM-enabled system.

Before you begin

You can access the Secure Service Container UI through the browser of your choice. To access the Secure Service Container UI, you need to have the following information.

- 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. However, if an administrator overwrote the HMC network settings through the UI **Networks** component for the installed appliance, you need to specify the IP address of the network adapter as specified in the UI component.
- You need to know the Administrator 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 **Maintenance** icon to display the **Invoke Installer** page.
2. Click **Installer**.
3. In the Description field, enter an optional description and click **Export**.

   The Installer exports the appliance configuration, which does not include runtime data from external storage devices.
4. Select **Save File** and click **OK** to save the exported configuration file to your file system.
5. On the **Confirm Invoke Installer** page, click **Yes** to continue.

Results

The installer is rebooted. How you access the Secure Service Container UI depends on the network settings that are in effect.

- If the network settings specified through the HMC are still the active settings, you are automatically routed to the **Login** page of the installer.
- If the HMC network settings were modified through the UI network management component (that is, overwritten within the installed appliance), you need to manually enter the HMC-specified IP address in your browser. 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.

Chapter 15. Moving an existing software appliance into a different Secure Service Container partition on the same system

Use this procedure to move an existing software appliance from one Secure Service Container partition to a new Secure Service Container partition on the same system. This action is a disruptive task. Also follow this procedure when you rename a Secure Service Container partition after you have already installed and run an appliance in it. 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 5 to enable N Port Identifier Virtualization (NPIV).
- The target FCP disks and FICON DASD must be large enough to fit the uncompressed appliance. Check the recommended size for the appliance before proceeding with installation.
- 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
- If you want to rename a Secure Service Container partition after you have already installed and run an appliance in it, you first need to stop the partition, rename it, and restart it *before* you follow this procedure for rebooting an appliance from an existing disk.

  On a standard-mode system

  1. Use the **Deactivate** task to stop the partition.
  2. Through image page for the partition in the **Customize/Delete Activation Profiles** task:
     a. In the **General** section, edit the name of the partition.
     b. In the **SSC** section, make sure that the Boot selection is set to **Secure Service Container installer**.
     c. Save your changes.
  3. Use the **Activate** task to restart the partition. The Secure Service Container installer is restarted.
  4. Continue with step “1” on page 64 of this procedure.

  On a DPM-enabled system

  1. Use the **Stop** task to stop the partition.
  2. Through the **Partition Details** task:
     a. In the **General** section, edit the short name of the partition.

b. In the **Boot** section, make sure that the **Boot in Installer Mode** switch is set to **YES**.

c. Save your changes.

3. Use the **Start** task to restart the partition. The Secure Service Container installer is restarted.
4. Continue with step "1" on page 64 of this procedure.

- 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. To securely identify the partition to which your browser is connected, make a note of the fingerprint and the client key that are also displayed in the Operating System Messages. For a sample display, see step "1" on page 64.
- You need to know the Administrator 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.

   To verify your SSL connection, you can compare the fingerprint or public key information that your browser provides to the information that you find in the Operating System Messages display. For example:

```
========================================================================
Fingerprint of SSC Installer web certificate, use this to verify
your client connections.
------------------------------------------------------------------------
Certificate:
subject=C = US, O = IBM, OU = zACI, CN = *.hostname
X509v3 Subject Alternative Name:
DNS:*.hostname, IP Address:192.0.2.0
SHA1 Fingerprint=4A:CE:4B:C6:C5:21:32:EC:39:D1:19:56:E2:3D:40:46:F3:CF:31:52
SHA256 Fingerprint=16:4E:E9:6A:7D:38:A0:C8:B2:65:98:85:66:AF:71:55:19:52:F8:FF:F
1:2F:61:85:2C:70:0E:07:8C:51:08:B6
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuhjx5iKYpWN0tz0jmNZd
4MSQZNGLZQtmcm4JzBpBn+Zv9nPC8N5b5wzgdwRXXeANwtk6BfVejj9C1AAMVRXT
GvrrziCw7ZrESqYhNsdoFE6LbrkaEIZyB2XuhbnrQN9n/YJwb8vQlV4RPM77ab/z
x765fNSIwAY+nCPJwACSuCORz5rg8zCc+xF/oWvMXMmaJ0EhXl+QaK6T56IA9NG8
owU0ubZXsTe6sf1VGE79M8DGr3T4C5/MVehCWa6InfK8dDJabgAG9pdzScBI0GrL
Bh0h19zHFQYaiwn/o7ZP6WFzQrC8FU541kwrlqVecNGO6x/qF6Qe3oQWBRo+CA9q
TwIDAQAB
-----END PUBLIC KEY-----
========================================================================
```

2. On the Login page, enter the Administrator 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) 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.

Note: For FICON DASD, only channel subsystem (CSS) 0 and subchannel set ID (SSID) 0-2 are supported. Also, make sure that you specify a four-character hexadecimal device number.

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. Both the WWPN and LUN must be 16-character hexadecimal numbers.

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 restart process begins, the installer displays the restart 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, if that is page is provided by the appliance.

6. If available, on the appliance page, complete the following steps.

a) If prompted by your browser, accept the self-signed certificate for the SSL connection.

To verify your SSL connection, you can compare the fingerprint or public key information that your browser provides to the information that you find in the Operating System Messages display. For example:

```
Certificate '192.0.2.0:4431:
subject=C = US, 0 = IBM, OU = ZACI, CN = * .hostname
X509v3 Subject Alternative Name:
DNS:*.hostname, IP Address:192.0.2.0
SHA1 Fingerprint=B5:1D:05:65:8C:E8:15:B8:17:06:14:1A:B9:2A: FB: 4E:61:7B:09:E0
- - - - -BEGIN PUBLIC KEY- - - - -
MIIBIJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA62JjRpF2cInQFcqHkXqb
INsyUIpDYoymv8FkFLrFdaG7aQpyjdl+JSasRSsfFVopi/sAOzhUfOiWCAaS8/SO
6fkebTVE5GSZObqF35Cttn79h6EKxhTutqxUV5hJ8eKS96ixoaYhw/LRG+eZ/HSf
JET5due7492VYMOeYUW03YOSZnzM7hMag93APAjpPomppArtgJeCJYOap20mtEwa
RIqdSi2zxe+yKd433CIgitJB5Ffq8oxm25eB1riw22fZ/GiFKbddmivnRa3rXSz2
zsOieywHwi8qk7BQbMh77tBX6mFRovrrk0h42+VLFjkpOTINm494tUPaibXy920K
```

```
nWIDAQAB
- - - - -END PUBLIC KEY- - - - -
```

b) Enter the administrator 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.

If a problem occurs, the installer displays an error message that can help you troubleshoot problems that are related to user input. If the message indicates an internal problem, see Appendix A, “Codes from the Secure Service Container installer,” on page 69.

Chapter 16. Migrating an appliance from one system to a new system

Use this procedure to migrate a Secure Service Container appliance from one system to another. You can migrate an installed appliance from one system to any other system on which you can configure a Secure Service Container partition. The suggested practice is to migrate appliances from one system model to the same model or a more recent model, with the same or a more recent level of firmware installed.

Before you begin

- To review the list of systems that support Secure Service Container partitions, and to find out where to get the latest available firmware for specific system models, see the appliance topics in Chapter 2, "Prerequisites for using Secure Service Container," on page 5.

  Notes:

  – Pay particular attention to the wrapping key ID information in Table 2 on page 6; the appliance wrapping key ID indicates whether the appliance can be decrypted and started on a given system.

  – If you are moving the appliance to a host system on which DPM R5.2 is installed, see "How the host system mode affects your planning and installation tasks" on page 6 for possible configuration tasks that you might need or want to complete on the new system.

- Make sure that you can log in to a Hardware Management Console (HMC) through which you can access the originating system and the new system.

About this task

This procedure contains steps that you need to perform on the originating system (where the appliance is currently installed) and steps to complete on the new system. Table 7 on page 67 provides an overview of these steps. To maximize availability of the appliance, make sure you complete each step in sequence.

Note: Depending on the appliance that you are migrating, you might need to complete additional steps that are not part of this procedure. Make sure that you also check the appliance documentation for any additional migration requirements.

Table 7. Overview of steps for migrating an appliance, using a new installation disk

Step number	Complete on the originating system	Complete on the new system
Step 1	—	Configure a new Secure Service Container partition.
Step 2	Export the configuration of the installed appliance that you are migrating.	—
Step 3	Deactivate (or stop) the Secure Service Container partition.	—
Step 4	—	Activate (or start) the Secure Service Container partition in Installer mode.
Step 5	—	Install the appliance in the Secure Service Container partition, using the new installation disk.
Step 6	—	Import the appliance configuration.

Procedure

1. On the new system, configure a Secure Service Container partition.

   Make sure that the storage devices and network connections for this new partition are based on the requirements of the appliance that you plan to migrate.

   The new system can be running in standard mode (that is, with Processor Resource/System Manager or PR/SM), or have IBM Dynamic Partition Manager (DPM) enabled. Use the appropriate instructions for the new system.

   - Chapter 3, “Configuring a Secure Service Container partition on a standard mode system,” on page 13
   - Chapter 8, “Creating a Secure Service Container partition on a DPM-enabled system,” on page 29
2. On the originating system, log in to the appliance, and use the Ex-/Import component to export the appliance configuration.

   For instructions, see “Exporting or importing appliance configuration data” on page 60.
3. Log in to an HMC through which you can access the originating system, and deactivate (or stop) the Secure Service Container partition on that system.

   Use the appropriate instructions:

   - Chapter 7, “Deactivating or deleting a Secure Service Container partition on a standard mode system,” on page 25
   - Chapter 12, “Stopping or deleting a Secure Service Container partition on a DPM-enabled system,” on page 41
4. On an HMC through which you can access the new system, start the new Secure Service Container partition, specifying the Secure Service Container Installer boot selection.

   Use the appropriate instructions:

   - Chapter 4, “Starting a Secure Service Container partition on a standard mode system,” on page 19
   - Chapter 9, “Starting a Secure Service Container partition on a DPM-enabled system,” on page 35
5. Install the appliance on the new system, following the instructions in Chapter 13, “Installing a new software appliance in a Secure Service Container partition,” on page 45.
6. Log in to the appliance, and use the Ex-/Import component to import the appliance configuration.

Appendix A. Codes from the Secure Service Container installer

If the Secure Service Container installer finds a problem that is not a client error, the installer returns an error message to indicate a server error. In this case, the UI displays a failure message. If the Call Home feature is enabled on the host system, the installer sends failure data to IBM for analysis.

Table 8 on page 69 lists the error codes that the installer can issue.

Table 8. Installer error reference codes

Error code	Description
2A5A0488	Detected an internal error related to the boot configuration file.
2A5A0490	Detected an error while attempting to read or modify the network configuration file.
2A5A0492	Detected an internal error related to reading appliance boot files.
2A5A0494	Detected an internal error related to uploading or installing a software appliance to a device.
2A5A0496	Detected an unexpected internal error.

Table 9 on page 69 lists the informational codes that the installer can issue.

Table 9. Installer informational reference codes

Informational code	Description
2A5A0481	Detected unexpected input or a timeout during the upload process. User should retry after checking input to the Secure Service Container installer.

Appendix B. Hardware feature codes

For systems prior to the IBM z16 (machine type 3931), you needed to order specific hardware feature codes to use the Linux Hosting Foundation or Container Hosting Foundation offerings.

Hardware feature codes enable unlimited right to use on IBM Z and LinuxONE systems (only for machine types 8561, 8562, 3907, 3906, 2965, and 2964). Depending on the type of applications that you intend to run in a Secure Service Container partition on one of those systems, you need to order one of the feature codes listed in Table 10 on page 71. These feature codes are mutually exclusive; each system can have only one of these Secure Service Container feature codes installed.

Table 10. Required hardware feature codes for Secure Service Container on prior systems

Feature codes	Secure Service Container and supported applications
0103	Linux Hosting Foundation: Supports the use of Secure Service Container, which is a specialized container for installing and running specific appliances:
0104	Container Hosting Foundation: Supports the use of Secure Service Container for IBM Cloud Private, which is a software appliance framework that is designed to securely host one or more Linux variable-use or container-based applications. For more information, see the Secure Service Container for ICP documentation in IBM Documentation at https://www.ibm.com/docs/en/sscfcp/1.1.0

Appendix C. 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.

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 or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names

might be trademarks of IBM or other companies. A current list of IBM trademarks is available on http://www.ibm.com/trademark.

JavaScript is a registered trademark of Oracle and/or its affiliates.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

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.

United Kingdom Notice

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce electromagnetic emissions to prevent interference to the reception of radio and television broadcasts.

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.

Japan Voluntary Control Council for Interference (VCCI) Notice

この装置は、クラス A 機器です。 この装置を住宅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 Electronics and Information Technology Industries Association (JEITA) Notice

（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：IBM Documentationの各製品の仕様ページ参照

This statement applies to products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

These statements apply to products greater than 20 A, single-phase.

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

These statements apply to products greater than 20 A per phase, three-phase.

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

People's Republic of China Notice

警告:在居住环境中,运行此设备可能会造成无线电干扰。

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.

Taiwan Notice

CNS 13438:

警告使用者：
此為甲類資訊技術設備，
於居住環境中使用時，
可能會造成射頻擾動，在此種情況下，
使用者會被要求採取某些適當的對策。

CNS 15936:

警告：為避免電磁干擾，本產品不應安裝或使用於住宅環境。

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

Electromagnetic Interference (EMI) Statement - Kingdom of Saudi Arabia Notice

قد يتسبب هذا المنتج في حدوث تداخل إذا تم استخدامه في المناطق السكنية.

ويجب تجنب هذا الاستخدام ما لم يتخذ المستخدم تدابير خاصة لتقليل الانبعاثات الكهرومغناطيسية لمنع التداخل مع استقبال البث الإذاعي والتلفزيوني.

تحذير: هذا الجهاز متوافق مع الفئة أ من SASO CISPR 32

في البيئة السكنية، قد يتسبب هذا الجهاز في حدوث تداخل لاسلكي.

Index

S

T

V

W

SC28-7062-00