STORAGETEK®

PART NUMBER	VERSION NUMBER	EDITION NUMBER
313463107	3.1	8

SVAA

SHARED VIRTUAL ARRAY ADMINISTRATOR

INSTALLATION, CUSTOMIZATION, AND MAINTENANCE FOR VM

PRODUCT TYPE
SOFTWARE

Shared Virtual Array Administrator

Version 3.1

for VM

Installation, Customization, and Maintenance

Part Number: 313463107

Eighth Edition (Rev H), March 2005 -- EC 132026

This edition applies to Shared Virtual Array Administrator (SVAA) for VM and to all subsequent modifications of that product until otherwise indicated in new editions or revision pages. If there are changes in the product or improvements in the information about the product, this document will be revised and reissued.

Comments concerning the contents of this document should be directed to:

Manager, Disk Storage Learning Products
Storage Technology Corporation
One StorageTek Drive
Louisville, CO 80028-2121

Contents

Figures

Tables

About This Book

SVAA is an optional software package that helps you configure, maintain, and track performance for the SVA subsystem. This book describes how to install the Shared Virtual Array Administrator (SVAA) software under the z/VM host operating system.

Notes:

1. Throughout this document, "VM" refers to **z/VM**, and "HCD" refers to either **HCD** or **IOCP**.
2. Whenever a host address is mentioned, the address referred to is **real**.
3. When a minidisk address is mentioned, the address referred to is **virtual**.

This book also describes how to install and maintain SVAA SnapShot, which is distributed as part of SVAA for VM. However, the SnapShot microcode must be installed on the SVA before you can perform snap operations. Contact your StorageTek service representative regarding microcode installation.

Who Should Read This Book

This book is for the systems programmers responsible for initializing and customizing SVAA in a VM operating system environment. It assumes that readers are familiar with the information contained in the *V2Xf Shared Virtual Array: Introduction*, *SVAA for VM Configuration and Administration*, and *SVAA for VM Reporting* manuals. It also assumes that readers are familiar with the VM operating system and the Interactive System Productivity Facility (ISPF).

Shared Virtual Array Documentation

This section lists both software documentation and hardware documentation for the Shared Virtual Array products.

How to Obtain Software Documentation

All of the Shared Virtual Array software publications are available:

- On the "SVA Software Publications" CD-ROM (part number 3134524*nn*). To order a copy, contact StorageTek Publication Sales and Service at 800-436-5554 or send a fax to 303-661-7367.
- Online (for viewing and printing), at the StorageTek Customer Resource Center (CRC) web site at: **www.support.storagetek.com**
  Click on Software and go to the Shared Virtual Array Software list.

  Note: Access to the CRC site requires a password. To obtain a password, call StorageTek Customer Support at 800-678-4430.

SVA Administrator Library:

SVA Administrator for VM

- *Shared Virtual Array Administrator for VM Configuration and Administration*
  3134629*nn*

- *Shared Virtual Array Administrator for VM Installation, Customization, and Maintenance* 3134631*nn*
- *Shared Virtual Array Administrator for VM Reporting* 3134630*nn*

SnapVantage (a feature of SVAA for VM)

- *SnapVantage Installation, Customization, and Usage Guide* 3134940*nn*

SVA Administrator for OS/390

- *Shared Virtual Array Administrator for OS/390 Configuration and Administration* 3112905*nn*
- *Shared Virtual Array Administrator for OS/390 Installation, Customization, and Maintenance* 3112908*nn*
- *Shared Virtual Array Administrator for OS/390 Reporting* 3112906*nn*
- *Shared Virtual Array SnapShot for OS/390 Installation, Customization, and Maintenance* 3112913*nn*

SVA Administrator for OS/390 and VM

- *Shared Virtual Array Administrator for OS/390 and VM Messages and Codes* 3112907*nn*

For any StorageTek Software:

- *Requesting Help from Software Support* 1121240*nn*

SVA Hardware Publications

Shared Virtual Array hardware publications are available:

- Online (for viewing and printing), at the StorageTek Customer Resource Center (CRC) web site at: **www.support.storagetek.com**
  Click on Disk Subsystems.

  Note: Access to the CRC site requires a password. To obtain a password, call StorageTek Customer Support at 800-678-4430.

V2Xf SVA Library:

- *V2Xf Shared Virtual Array General Information* MO9216*x*

- *V2Xf Shared Virtual Array Introduction*
  MO9217*x*
- *V2Xf Shared Virtual Array Operation and Recovery*
  MO9219*x*
- *V2Xf Shared Virtual Array Planning*
  MO9218*x*
- *V2Xf Shared Virtual Array Reference*
  MO9220*x*
- *V2Xf Shared Virtual Array System Assurance*
  MO9221*x*
- *V2Xf Shared Virtual Array Peer-to-Peer Remote Copy Configuration Guide (PPRCFCN)*
  MO9211*x*

V2X SVA Library:

- *V2X Shared Virtual Array General Information*
  MO9134*x*
- *V2X Shared Virtual Array Introduction*
  MO9135*x*
- *V2X Shared Virtual Array Operation and Recovery*
  MO9137*x*
- *V2X Shared Virtual Array Planning*
  MO9136*x*
- *V2X Shared Virtual Array Reference*
  MO9139*x*
- *V2X Shared Virtual Array System Assurance*
  MO9138*x*

V960 SVA Library:

- *V960 Shared Virtual Array General Information*
  MO5011*x*
- *V960 Shared Virtual Array Introduction*
  MO5006*x*

- *V960 Shared Virtual Array Operation and Recovery* MO5007*x*
- *V960 Shared Virtual Array Planning* MO5008*x*
- *V960 Shared Virtual Array Reference* MO5009*x*
- *V960 Shared Virtual Array System Assurance* MO5010*x*

Peer-to-Peer Remote Copy for V2X, V2X2, and V960:

- *Peer-to-Peer Remote Copy Configuration Guide* MP4007*x*

Trademarks

The following terms are trademarks or registered trademarks of Storage Technology Corporation:

- Iceberg
- Shared Virtual Array
- SnapVantage
- StorageTek
- SVA

The following terms are trademarks or registered trademarks of International Business Machines Corporation:

- DFSMS/MVS
- DFSMS/VM
- ESCON
- FICON
- IBM
- MVS
- OS/390
- RACF
- RMF
- VM/ESA
- z/OS
- z/VM

The following terms are trademarks or registered trademarks of Microsoft Corporation:

- DOS
- Excel
- Windows

The following terms are trademarks or registered trademarks of SAS Institute, Incorporated:

- SAS
- SAS/C
- SAS/GRAPH

UNIX is a registered trademark of The Open Group.

Note: Other terms and product names used herein may be trademarks of their respective owners.

Product Support

StorageTek Customer Services provides 24-hour assistance for questions or problems related to StorageTek products. Calls from our customers receive immediate attention from trained diagnostic specialists. Call 800-678-4430.

Refer to the document *Requesting Help from Software Support* for detailed information about contacting StorageTek for technical support in your country or geographical location.

During problem resolution, Software Support may request that you provide specific diagnostic materials. Although printed data might be acceptable, data in machine-readable form is much preferred.

VM Diagnostic Materials

Software Support may request one or more of the following kinds of diagnostic materials, depending on the nature of the problem:

- Details of the circumstances in which the problem occurred
- Console logs
- EREP type 'S' records
- ISPF panel images
- ISPF panel names and SPFLOG
- CCW I/O trace (TRSOURCE) output
- VMDUMP data
- CP dump data
- Listings of SVAA files altered during installation, including the PROFSIBS and PROFSIBA macros
- Copies of logging files

Summary of Changes

Eighth Edition (Rev H), March 2005 EC 132026

This edition:

- Updates the Software Prerequisites in Chapter 2 with new minimum levels.
- Adds some information on how to make changes to the SYSPROF EXEC to Step 21 in Chapter 4.

Seventh Edition (Rev G), April 2004 EC nnnnnn

This edition:

- Updates CP QUERY authorization in Step 6.
- Removes references for VM/ESA.
- Updates Step 23 and setting the missing-interrupt handler timeout value.

All lines containing significant changes are identified by vertical bars in the left margin.

Sixth Edition (Rev F), November 2003 EC 128861

This edition:

- Documents SVAA changes introduced with the release of the V2Xf SVA which supports only FICON connections.
- Includes the term “Detached Operator Panel” or “DOP” wherever the Local Operator Panel or LOP is mentioned
- Contains minor corrections and edits throughout this document.

All lines containing significant changes are identified by vertical bars in the left margin.

Fifth Edition (Rev E), June 2003 EC 128585

This edition:

- Includes updates to the output from the SnapShot installation verification test in Step 14.
- In Step 15, adds information regarding SIM processing and automated operations facilities.
- Contains minor corrections and edits throughout this document.

All lines containing significant changes are identified by vertical bars in the left margin.

Fourth Edition (Rev D), October 2002 EC 128585

This edition:

- Describes additional VM privileges in Step 6.
- For V2X, revises the virtual storage numbers specified for STKSRP in Step 9.
- In Step 22, adds a description of SIBDEFDV—a sample SVAA macro for defining and initializing SVA devices.

All lines containing significant changes are identified by vertical bars in the left margin.

Third Edition (Rev C), June 2002 EC 128518

This edition:

- Adds mention of SnapVantage—a new feature of SVAA that enables rapid deployment and easy management of virtual Linux servers under z/VM. A new step (Step 3) in Chapter 2 lists additional preparation necessary for installing SnapVantage. (Adding this step causes steps 3 through 23 in previous editions to be renumbered to 4 through 24.)
- Revises information in Steps 6, 10, and 11.
- Adds notes in Step 17 about downloading SVAA maintenance PTFs from StorageTek's Customer Resource Center site.
- In Appendix A, describes seven new files in the SIBSAMP MACLIB.
- Makes additional minor updates.

Second Edition (Rev B), January 2002 EC 123350

This edition:

- Changes the recommended MIH (missing interrupt handler) timeout value to 4 minutes, 30 seconds in Step 22 (page 5-3).

Chapter 1. Installation Summary and Checklist

This chapter contains a checklist summarizing the steps required to install SVAA in a VM operating environment.

You can install SVAA before or after your SVA hardware is installed. If you install SVAA before your SVA hardware is installed, you can use the Reporter functions of SVAA to collect statistics and generate reports for any non-SVA devices you have defined to SVAA.

Note: The SnapShot software is distributed as part of SVAA for VM. However, the SnapShot microcode must be installed on the SVA before you can perform snap operations. Contact your StorageTek service representative regarding microcode installation.

Use the checklist in Table 1-1 to ensure that you complete all the required steps for installing SVAA. This table also lists any optional steps you may want to perform.

Table 1-1 (Page 1 of 2). *Installation checklist*

Step	Description of action	Required or optional?	Page	√
	Planning for SVAA Installation			
1	Verify that installation materials are available and the prerequisite software is installed.	Required	2-2	
2	Make decisions about how you want to use Reporter.	Optional	2-2	
3	Plan for the SnapVantage feature.	Optional	2-3	
4	Plan for SVAA and VM security.	Required	2-3	
	Installing SVAA			
5	Define SVA to VM (even if you have not yet installed the SVA hardware).	Required	3-2	
6	Define VM privileges for SVAA.	Optional	3-3	
7	Check to see whether the StorageTek maintenance virtual machine has been defined. If it has not, define this user ID.	Required	3-4	
8	Define the $SUBSYS$ user ID.	Optional	3-6	
9	Define the Reporter user ID.	Optional	3-10	
10	Format the SVAA minidisks using the CMS FORMAT command.	Required	3-12	
11	Check the contents of the Product Tape.	Required	3-12	
12	Review SVAA FMIDs.	Required	3-13	
13	Load the SVAA Software.	Required	3-13	
14	Run the Installation Verification Test.	Optional	3-16	

Table 1-1 (Page 2 of 2). *Installation checklist*

Step	Description of action	Required or optional?	Page	√
15	Review Special Considerations.	Required	3-18	
16	Define SVAA's DisContiguous Saved Segment (DCSS)	Optional	3-19	
17	Apply Maintenance.	Required	3-21	
	Customizing the SVAA Installation			
18	Customize the ISPF panel for the SVAA software.	Optional	4-2	
19	Customize the default SVAA profile.	Optional	4-4	
20	Customize Reporter to meet your company's needs.	Optional	4-6	
21	Customize the SYSPROF EXEC.	Optional	4-11	
	Using SVAA			
22	Establish communications between SVAA and SVA.	Required	5-2	
23	Use the CP SET MITIME command to change the default VM missing-interrupt handler timeout value for DASD.	Required	5-3	
24	Use SVAA to configure and report on SVA subsystems.	Required	5-4	

Chapter 2. Planning for SVAA Installation

Pre-installation planning consists of the following tasks (which are detailed in this chapter):

Step 1 Verify that all installation materials are available

Step 2 Plan for SVAA Reporter (optional)

Step 3 Plan for SnapVantage feature (optional)

Step 4 Plan security measures

Step 1: Verify Installation Materials and Software Prerequisites (Required)

First, make sure that you have all installation materials. In addition to this manual, StorageTek provides the following materials:

- SVAA Product tape and Maintenance tape
- SVAA documentation:
  - *SVAA for VM Configuration and Administration*
  - *SVAA for VM Reporting*
  - *SVAA for OS/390 and VM Messages and Codes*
- SnapVantage documentation (optional):
  - *SnapVantage Installation, Customization, and Usage Guide*

After you have verified the installation materials, make sure that your system has the necessary software prerequisites. SVAA for VM requires the minimum software releases listed in Table 2-1.

Table 2-1. *System Software Prerequisites*

Category	Description	Minimum Level
Operating System Software	z/VM	Version 3.1
Dialog Support	ISPF	Version 3.5
Report Software	SAS	Version 6.07

Note: SnapShot is distributed with SVAA for VM. However, the SnapShot microcode must be installed on the SVA before you can perform snap operations. Contact your StorageTek service representative regarding microcode installation.

Step 2: Plan for SVAA Reporter (Optional)

If you will collect data with Reporter, consider the following issues:

- If you have multiple hosts using the SVA subsystem, only one Reporter data collection task needs to be defined. The performance data for all functional volumes is available to any host that has access to the SVA subsystem.
- In Step 9 on page 3-10, you will allocate the DASD that will contain Reporter's collected data. Refer to the *SVAA for VM Reporting* manual for information about estimating your data storage requirements.
- For Reporter data collection, you can specify an alternate minidisk to log data if your main logging minidisk fills up. Refer to the *SVAA for VM Reporting* manual for information about specifying main and alternate logging files.

Step 3: Plan for SnapVantage Feature (Optional)

If you plan to manage guest Linux Servers with SnapVantage, you need to take the following additional steps:

- Apply the latest SVAA Maintenance PTFs.
- Obtain the *SnapVantage Installation, Customization, and Usage Guide*.
- Obtain a SnapVantage license key.

Step 4: Plan System Security (Required)

Before installing SVAA, there are a number of security issues you should consider.

User Access to SVAA

You usually install the SVAA run-time software on the MAINTSTK[1] 454 minidisk. If you have a VM security product (such as RACF or VMSECURE), you may need to update your database to control user access to this minidisk. For example, the STKSRP[2] user ID requires access to SVAA. See Step 7 on page 3-4 for information about defining the MAINTSTK user ID. See Step 9 on page 3-10 for information about defining the STKSRP user ID.

VM Privilege Classes for SVAA

SVAA requires only privilege Class G for normal operation. Several SVAA subcommands, however, require additional authorizations. Step 6 on page 3-3 provides detailed information on the exceptions.

User Access to SVA

SVAA uses StorageTek's Extended Control And Monitoring (ECAM) protocol to communicate with the SVA. When you define an SVAA functional device, you designate the device as either a *privileged* or *non-privileged* ECAM device. If you specify a privileged ECAM device for communications, you can issue configuration and control commands to an SVA subsystem. If you specify a non-privileged ECAM device for communications, you can issue Query commands to an SVA subsystem which can return information (such as Reporter reports).

In Step 8 on page 3-6, you will define the $SUBSYS$ user ID with minidisks that map to the ECAM devices used for communications. You can use a VM security product to control user access to these minidisks and, therefore, the user's ability to query and configure the SVA.

---

[1] MAINTSTK is the default user ID of the virtual machine that contains SVAA's VM programs and maintenance materials. This manual calls this virtual machine MAINTSTK.

[2] STKSRP is the default user ID of the SVAA data collection service machine. This manual calls this virtual machine STKSRP.

Chapter 3. Installing SVAA

Installing SVAA consists of the following tasks (which are detailed in this chapter):

Step 5 Define the SVA subsystem to VM

Step 6 Define VM privileges

Step 7 Define the MAINTSTK User ID

Step 8 Define the ECAM Communication Device

Step 9 Define the STKSRP User ID

Step 10 Format the SVAA minidisks

Step 11 Check the contents of the product tape

Step 12 Review SVAA FMIDs

Step 13 Load the SVAA software

Step 14 Run the installation verification test

Step 15 Review special considerations

Step 16 Define SVAA's DisContiguous Saved Segment

Step 17 Apply Maintenance

Step 5: Define the SVA to VM (Required)

To define the SVA subsystem to VM, you should complete the following tasks:

- Make real I/O definitions for SVA functional devices
- Run the I/O configuration program

For information about completing these tasks, refer to the following publications:

- StorageTek *V2Xf Shared Virtual Array: Planning* guide
- IBM *z/VM CP Planning and Administration*
- IBM *Input/Output Configuration Program User's Guide*

Step 6: Define VM Privileges (Optional)

Most SVAA functions are available to a General User (privilege Class G) with access to an SVA ECAM device. This section describes exceptions for certain subcommands that require additional privileges to be configured for the SVAA privileged user.

CP Command Authorizations

Class B CP QUERY

SVAA device mapping uses the Class B CP QUERY DASD and CP QUERY PAV commands to display host DASD. Without device mapping enabled, SVAA will report blank values for host volsers and unit addresses.

Class A CP DEFINE MDISK and Class B CP ATTACH

The SVAA SNAP VOLUME subcommand requires CLASS A CP DEFINE MDISK and CLASS B CP ATTACH to set up and perform the SnapShot operation. The SNAP VOLUME subcommand is intended for **VM disk storage administrators only**.

CP DIAGNOSE CODE Authorizations

CP DIAGNOSE code X'0E4'

The SVAA QUERY MINIDISK subcommand requires the use of the CP DIAGNOSE code X'0E4'.

CP DIAGNOSE code X'25C'

The SVAA LIST MINIDISK subcommand requires the use of CP DIAGNOSE code X'25C'.

The following user directory options obtain authorization for both of these DIAGNOSE codes:

```
OPTION DEVINFO DEVMAINT
```

CP Class Override Feature

CP provides the ability for the administrator to override certain commands for individual users. For example, you may want to define a new privilege class S, for SVAA users as in one of the following examples.

- In the System Configuration file (recommended):

```
MODIFY CMD QUERY IBMCLASS B PRIVCLASS BS
MODIFY CMD DIAG25C IBMCLASS B PRIVCLASS BS
```

- In the Class Override file:

```
QUERY IBMCLASS=B NEWCLASS=BS
DIAG25C IBMCLASS=B NEWCLASS=BS
```

Notes:

1. See the appropriate IBM documentation for a complete description of these VM privileges and commands.
2. Use CP QUERY COMMANDS to display the authorized CP commands and DIAGNOSE codes for a user.
3. If you are using an External Security Manager, there may be additional authorizations required from the vendor.

Step 7: Define the MAINTSTK User ID (Required)

If your system already has a MAINTSTK user ID, you do not need to define minidisk 191. However, you should make sure minidisk 191 has sufficient space available for both SVAA and your other software products. You should also specify a minimum of 16 megabytes of virtual storage for the MAINTSTK user ID.

Table 3-1 describes the attributes of the SVAA minidisks defined to the MAINTSTK userid.

Table 3-1. *Target Minidisks*

Disk name	Minidisk CUU	Minidisk Label	3380 Cylinders	3390 Cylinders	Usage Note
ADISK	191	STK191	12	10	(1)
BASE	450	IHBASE	60	50	
DELTA	451	IHDELT	60	50	
MERGE	452	IHMERG	30	24	
ZAP	453	IHSZAP	1	1	
RUN	454	IHSRUN	60	50	

Usage Notes:

(1) The ADISK may contain files for other software products. These values represent additional space requirements for installation of SVAA.

The values specified in the *3380 Cylinders* and *3390 Cylinders* columns of the table are the recommended allocation size for each of the minidisks. This includes additional space for configuration and maintenance of the product.

Figure 3-1 shows an example of a MAINTSTK VM directory entry for SVAA.

```
USER MAINTSTK password 16M 32M G[E]
ACCOUNT xxxxxx
*
IPL CMS PARM AUTOCR
CONSOLE 009 3215 A
SPOOL 00C 2540 READER *
SPOOL 00D 2540 PUNCH A
SPOOL 00E 1403 A
*
LINK MAINT    190 190 RR
LINK MAINT    19D 19D RR
LINK MAINT    19E 19E RR
*
MDISK 191 devtype scyl cyls volser MR rpw wpw mpw
MDISK 450 devtype scyl cyls volser MR rpw
MDISK 451 devtype scyl cyls volser MR rpw
MDISK 452 devtype scyl cyls volser MR rpw wpw mpw
MDISK 453 devtype scyl cyls volser MR rpw
MDISK 454 devtype scyl cyls volser MR rpw
```

Figure 3-1. *Example of MAINTSTK VM directory entry for SVAA*

Example of MAINTSTK Directory Statements for SVAA

The MAINTSTK directory statements for SVAA are:

USER MAINTSTK *password* **16M 32M G[E]**
The default virtual storage is 16 megabytes and the maximum is 32 megabytes. MAINTSTK needs only Class G for normal operation. Class E is required if an SVAA saved segment is desired.

MDISK statements
In these statements, specify:

- The device type (3380 or 3390) for the *devtype* variables
- Starting cylinder addresses for the *scyl* variables
- Sizes of the minidisks for the *cyls* variables
- Volume serial IDs for the *volser* variables

Note: If you have a directory maintenance product, you may need to update your database to define these new minidisks and to allow users to access the SVAA run-time software on minidisk 454.

Table 3-2 describes each minidisk.

Table 3-2. *MAINTSTK minidisks*

CUU	Disk Name	Description
191	ADISK	A-disk for the installation and service programs.
450	BASE	Minidisk that contains the original product files from the installation tape.
451	DELTA	Minidisk that contains the PTFs for the service programs.
452	MERGE	Minidisk that contains the PTFs that have been applied.
453	ZAP	Minidisk that contains files that have been copied from the BASE or MERGE disks and have had bug fixes applied (have been zapped).
454	RUN	Minidisk that contains all files necessary to run the SVAA product. It contains: • All MODULE files • All ISPF libraries • All non-installation EXECs • All sample materials • All LOADLIB files • All SAS/C run-time libraries

Step 8: Define the ECAM Communication Device (Required)

It is recommended that you define your ECAM communication devices using a "nolog" user ID (called $SUBSYS$ in this manual) with minidisk definitions for the following:

- Any SVAA ECAM devices that you will use for communications with SVA subsystems.
- Any non-SVA subsystems for which you want Reporter to collect data.

Figure 3-2 on page 3-7 shows an example of a $SUBSYS$ VM directory entry.

Defining Minidisks for ECAM Devices

Using a minidisk definition for an ECAM device lets multiple SVAA users communicate with the SVA over the same host device address. An ECAM minidisk must be available to SVAA in **write** mode and must include real cylinder 0 in its definition. SVAA doesn't actually write data to the minidisk. It uses a write data channel command to send requests to the SVA.

Note: Non-SVA subsystems reject SVA ECAM requests since these non-SVA subsystems do not recognize the ECAM communication protocol.

Defining Non-SVA Devices

Reporter can also collect performance data from 3990 subsystems. You must define at least one minidisk on each subsystem for which you want Reporter to collect data; this gives Reporter a virtual device address over which it can collect the performance data. Reporter requires only read access to these minidisks, and you can specify any starting cylinder.

In the example in Figure 3-2, multiple minidisks are defined for each SVA and non-SVA subsystem. This allows SVAA to select an available I/O path to each subsystem. To use these MDISK statement examples, specify volume serial IDs for the *volser* variables.

Note: An ECAM device is used for SVAA communications but may also contain user data. When setting up an ECAM device that will be shared with other virtual (or real) machines refer to the VM rules for shared DASD. For most situations, user IDs linking to SVA ECAM minidisks need to link in MW mode. User IDs linking to non-SVA minidisks only need to link in RR mode.

```
USER $SUBSYS$ NOLOG 1M 1M G
ACCOUNT xxxxxx
*
********* SVA Subsystem SUBSYSA ********
MDISK 200 3380 0000 0001 volser MW rpw wpw mpw
MDISK 201 3380 0000 0001 volser MW rpw wpw mpw
*
********* SVA Subsystem SUBSYSB ********
MDISK 210 3390 0000 0001 volser MW rpw wpw mpw
MDISK 211 3390 0000 0001 volser MW rpw wpw mpw
MDISK 212 3390 0000 0001 volser MW rpw wpw mpw
*
********* Non-SVA SSID 0010 ********
MDISK 300 3390 0000 0001 volser RR rpw
MDISK 301 3390 0100 0001 volser RR rpw
*
********* Non-SVA SSID 0020 ********
MDISK 310 3390 0000 0001 volser RR rpw
MDISK 311 3390 0500 0001 volser RR rpw
```

Figure 3-2. *Example of $SUBSYS$ VM directory entry*

SVAA Device Mapping

SVAA device mapping associates an SVA functional device identifier (FDID) with a host device address and volser. For device mapping to be in effect, you must issue the SET DEVICEMAP(ON) subcommand (documented in the *SVAA for VM Configuration and Administration* manual).

The key to the device mapping scheme for an SVA subsystem is the ECAM device that you define by means of the SET ECAMDEVICE subcommand (documented in the *SVAA for VM Configuration and Administration* manual). You may need to define multiple ECAM devices, as noted below.

Notes:

1. Whenever a host address is mentioned, the address referred to is **real**.
2. When a minidisk address is mentioned, the address referred to is **virtual**.

VM host device mapping information is collected by:

1. Obtaining the ECAM device's host device address from the virtual device address (CP DIAGNOSE code X'0E4').
2. Obtaining the SVA channel definition for the host device address. This provides the boundaries of the channel interface: the interface ID, the device address range defined to the interface, and the base FDID.
3. Combining this information to create a host view of the device configuration within the SVA subsystem.

The number of devices you specify in the SET ECAMDEVICE subcommand depends upon the range of host addresses defined to each channel interface. The following configurations are examples.

All devices defined in one contiguous range:

If the host configuration defines all devices in a contiguous range for each channel interface, the SVA channel interface definition should accurately reflect the device range of the host, and a single ECAM device can recognize all host devices.

Example 1. For a 1024-device SVA subsystem:
In the following channel configuration, with all devices in a contiguous range of 0 to 1023 and host device addresses C000 to C3FF,

```
Interface  Base          Address
    ID     FDID    FDID   Range
   ----    ----    ----   -----
    A       00      00    1024
    B       00      00    1024
    C       00      00    1024
    D       00      00    1024
```

define one ECAM device:

```
SET ECAMDEVICE (C000)
```

Example 2. For a 4096-device SVA subsystem:
In this configuration, the host addresses are contiguous and range from 7000 to 7FFF using volsers SV7000-SV7FFF. Define an ECAM device with an MDISK statement and enable it using the SVAA SET ECAMDEVICE subcommand, define one ECAM device:

```
VM Directory:  MDISK  7000 3390 0000 0001 SV7000 MW
PROFSIBA SIB macro:  SET ECAMDEVICE (7000)
```

Devices defined in four non-contiguous ranges:

If the host configuration defines four non-contiguous 3990 control unit address ranges—one range of addresses for each channel interface, the SVA channel interface definition should accurately reflect the device range of the host, and multiple ECAM devices are required to recognize all host devices. That is, you need to define at least one ECAM device for each channel interface.

Example 3. For a 256-device SVA subsystem:
In the following channel configuration of four non-contiguous control unit address ranges of 64 devices each, defined at 200, 340, 480, and 5C0,

```
Interface  Base          Address
    ID     FDID    FDID   Range
   ----    ----    ----   -----
    A       00      00     064
    B       40      40     064
    C       80      80     064
    D       C0      C0     064
```

define four ECAM devices:

```
SET ECAMDEVICE (200 340 480 5C0)
```

Each ECAM minidisk is linked to your virtual machine, and the virtual addresses are placed in the SET ECAMDEVICE subcommand in your PROFSIBA SIB macro.

Example 4. For a 1024-device SVA subsystem:
In the following channel configuration of four non-contiguous control unit address ranges of 256 devices each, defined at 100, 700, A00, and 1300,

Interface ID	Base FDID	FDID	Address Range
A	00	00	256
B	100	100	256
C	200	200	256
D	300	300	256

define four ECAM devices:

```
SET ECAMDEVICE (100 700 A00 1300)
```

Each ECAM minidisk is linked to your virtual machine, and the virtual addresses are placed in the SET ECAMDEVICE subcommand in your PROFSIBA SIB macro.

Step 9: Define the STKSRP User ID (Optional)

Although this step is optional, it is required if you want to use Reporter. In this step, you define the STKSRP user ID that will collect both SVA and non-SVA performance data. Performance data for an entire SVA subsystem can be collected by a single host. If you are operating in a multi-host environment, the performance Data Collection Task should be executed on only one host.

Figure 3-3 shows an example of an STKSRP VM directory entry.

```
USER STKSRP password 32M 64M G[B]
ACCOUNT xxxxxx
*
IPL CMS
*
* Authorized IUCV connections
IUCV ALLOW MSGLIMIT 255
*
CONSOLE 009 3215 A
SPOOL 00C 2540 READER *
SPOOL 00D 2540 PUNCH A
SPOOL 00E 1403 A
*
LINK MAINT    190 190 RR
LINK MAINT    19D 19D RR
LINK MAINT    19E 19E RR
LINK MAINTSTK 454 192 RR
*
MDISK 191 devtype scyl cyls volser MR rpw wpw
MDISK 196 devtype scyl cyls volser MR rpw wpw
```

Figure 3-3. *Example of STKSRP VM directory entry*

Example of STKSRP Directory Statements

The STKSRP directory statements are:

USER STKSRP *password* **32M 64M G[BE]**
: The default virtual storage is 32 megabytes and the maximum is 64 megabytes.

  STKSRP needs only Class G for normal operation. See Step 6 on page 3-3 for device mapping and Class B CP QUERY considerations.

IUCV ALLOW MSGLIMIT 255
: Specifies that any user ID can request connection to STKSRP. See Step 20D on page 4-10 for information about authorizing users for Reporter services.

LINK MAINTSTK 454 192 RR
: CP link to the MAINTSTK 454 minidisk that contains the SVAA run-time software.

  Note: If you have a VM security product (such as RACF), you may need to update your database to let STKSRP access the SVAA run-time software on the MAINTSTK 454 minidisk.

MDISK statements

Define the following Reporter minidisks:

191 Contains files customized by the installation. You should allocate at least 5 cylinders for this minidisk.

196 Contains data collected by STKSRP. Refer to the *SVAA for VM Reporting* manual for the data storage requirements for this minidisk.

In these statements, specify:

- The device type (3380 or 3390) for the *devtype* variables
- Starting cylinder addresses for the *scyl* variables
- Sizes of the minidisks for the *cyls* variables
- Volume serial IDs for the *volser* variables

Step 10: Format Minidisks (Required)

In this step, you format the minidisks that you defined for the MAINTSTK and STKSRP user IDs in Step 7 and Step 9.

To format MAINTSTK's minidisks:

1. Log on to MAINTSTK.
2. If you defined the 191 minidisk in Step 7, use the CMS FORMAT command to format this minidisk with a mode of A and a label of STK191.
3. The other minidisks listed in Table 3-3 will be automatically formatted by the install exec procedure.

Table 3-3. *MAINTSTK minidisk formatting values*

Virtual address	Mode	Label
450	B	IHBASE
451	C	IHDELT
452	D	IHMERG
453	E	IHSZAP
454	F	IHSRUN

To format STKSRP's minidisks:

1. Log on to STKSRP.
2. Format the 191 and 196 minidisks with the values shown in Table 3-4.

Table 3-4. *STKSRP minidisk formatting values*

Virtual address	Mode	Label
191	A	any label
196	any mode	any label

Step 11: Check the Contents of the Product Tape (Required)

SVAA for VM Version 3.1 is contained on one nonlabeled tape in VMFPLC2 format. You can verify its contents by using the VMFPLC2 SCAN command.

The tape contains the following files.

File Number	Disk name	Contents
1	ADISK	Tape installation and maintenance files
2	BASE	Base product files
3	DELTA	Initial delta files
4	MERGE	Initial merge files
5	ZAP	Initial zap files
6	RUN	Product runtime files

Step 12: Review SVAA FMIDs (Required)

The SVAA software product is packaged in VMFPLC2 format along with selected components of the SAS/C run-time library. SVAA Version 3.1 has the following product FMIDs:

SSIB310V SVAA product library

SSOC210V SVA SnapShot for VM

SSNI210V SVA Low Level API

SSKP124V Common parser library

Each FMID has an associated VMFPARM file (product parameter file). You must keep the VMFPARM minidisk definitions synchronized with the product's FMIDs.

Step 13: Load the SVAA Software (Required)

Warning: If a previous version of SVAA or IXFP for VM is installed on the same minidisk addresses defined in the VMFPARM file, ensure a current backup of the previous version exists or assign different minidisk addresses in the VMFPARM files

To load the SVAA software:

1. Log on to the MAINTSTK user ID.
2. Attach a tape drive as virtual device 181.
3. Mount the SVAA installation tape on virtual device 181.
4. To load the installation EXEC and its parameter files on the A-disk, enter the following commands:

```
ACCESS 191 A
VMFPLC2 REW
VMFPLC2 LOAD * * A
```

5. Review the README SSIB310V file that has been loaded to the A-disk. This file contains information about the installation process as well as new features and functions.
6. Modify the file SSIB310V VMFPARM if desired. This file contains minidisk address definitions required for SVAA installation. Figure 3-4 shows the section of SSIB310V VMFPARM that contains these address definitions. You can change the addresses, but **do not** change the minidisk names.

   Warning: Any minidisk address changes made to the file SSIB310V VMFPARM must also have equivalent changes made to the file SSKP124V, SSNI210V, and SSOC210V VMFPARM files.

```
*
*       Shared Virtual Array Administrator
*        (PRODUCT=1127-008, ID=SSIB310V)
*
* Maintenance service machine minidisk definitions
*
* WARNING:  Keep definitions in-sync with SSKP124V, SSOC210V, SSNI210V
*
*
ADISK     191
BASE      450
DELTA     451
MERGE     452
ZAP       453
RUN       454
```

Figure 3-4. *File SSIB310V VMFPARM A*

7. To load the rest of the product files, enter the following command:

   EXEC ISSIB310

   The installation EXEC takes about 5 to 10 minutes to load the product files and displays progress messages as each group of files is loaded. Figure 3-5 on page 3-15 shows examples of these messages.

```
This program will remove ALL files residing on the
disks defined in the parameter file, SSIB310V VMFPARM
A as BASE 450, DELTA 451, MERGE 452, ZAP 453, and RUN 454.

Do you wish to continue.  (Yes | No)
yes
******************************************
*** Loading install tape for           ***
*** Storage Technology Corporation     ***
*** Product FMID:  SSIB310V            ***
***                                    ***
*** Shared Virtual Array Administrator ***
***            Release V3.1            ***
***                                    ***
******************************************
TIME IS 09:45:04 MDT MONDAY 04/09/01
CONNECT= 00:09:50 VIRTCPU= 000:00.10 TOTCPU= 000:00.21
ISSIB310:  Loading files from product tape to BASE disk.
ISSIB310:  Loading files from product tape to DELTA disk.
ISSIB310:  Loading files from product tape to MERGE disk.
ISSIB310:  Loading files from product tape to ZAP disk.
ISSIB310:  Loading files from product tape to RUN disk.

ISSIB310:  All files have been loaded from tape for SSIB310V
******************************************
*** ISSIB310 has completed processing for ***
*** Storage Technology Corporation     ***
*** Product FMID:  SSIB310V            ***
***                                    ***
*** Shared Virtual Array Administrator ***
***                                    ***
******************************************
TIME IS 09:48:02 MDT MONDAY 04/09/01
CONNECT= 00:12:48 VIRTCPU= 000:02.08 TOTCPU= 000:04.67
Ready;
```

Figure 3-5. *Messages displayed during installation*

Note: After these steps have been completed, you will have installed SnapShot also. SnapShot is packaged as a part of SVAA for VM. However, the SnapShot microcode must be installed on the SVA before you can perform snap operations. Contact your StorageTek service representative regarding microcode installation.

Step 14: Run the Installation Verification Test (Optional)

Running the Installation Verification Test (IVT), which is optional, lets you verify that you have successfully installed the SVAA software.

To run the IVT:

1. Log on to MAINTSTK if you are not already logged on.
2. If required, access the 454 minidisk that contains the SVAA run-time software.
3. Link to one of the ECAM devices (minidisks), in write mode, that you defined in Step 8 on page 3-6. For example, enter the following command:

   CP LINK $SUBSYS$ 200 300 MW

4. To run the IVT, enter the following command:

   EXEC VSSIB310

5. The EXEC prompts you for the address of an ECAM device. Enter the address of the device that you linked to in Step 3 above. For example, enter:

   300

6. The EXEC prompts you for the Reporter user ID. Enter the Reporter user ID; the default is STKSRP.
7. The following is an example of what the EXEC displays:

```
Subsystem name:              unknown
Subsystem serial no.:        unknown
ECAM device:                 300
Count of ECAM devices:       unknown
Count of Non-ECAM devices:   unknown
Subsystem reporter status:   Disabled
Ready;
```

   As the example above shows, if you run the IVT immediately after loading the software, the IVT displays messages that report SVA subsystems and ECAM devices as unknown and Reporter as disabled.

   You may also want to run the IVT after completing the “Customizing Reporter” and “Establishing Communications Between SVAA and SVA” steps. Here is an example of what the EXEC displays with the SVA subsystem installed and communications with SVAA set up:

```
Subsystem name:              SUBSYS01
Subsystem serial no.:        88888888
ECAM device:                 300
Count of ECAM devices:       1
Count of Non-ECAM devices:   0
Subsystem reporter status:   Disabled
```

8. Next, the EXEC asks whether you want to execute SnapShot. Figure 3-6 shows examples of the messages issued during this phase of the installation verification.

```
Checking for IF Feature on Subsystem: SUBSYS01
SVA Instant Format is supported on SUBSYS01

Do you want to execute a SnapShot command?  (Yes|No)

y
A SNAP MINIDISK subcommand will be executed.
The SnapShot feature must be enabled in the subsystem.
Enter a SOURCE virtual device address or QUIT to exit.
302

<<<<<<<<<< WARNING >>>>>>>>>>
The target device will be overwritten with source data.

Enter a TARGET virtual device address or QUIT to exit.
301
SIB4791D   Snap 15 cylinders from DONJ 302 0-14 to DONJ 301 0-14?
SIB4791D   Reply YES to continue or NO to cancel the subcommand.
SIBADMIN:
yes
SIB4617I   14:19:19 SnapShot completed, rc=0.
RE-ACCESSing target minidisk 301

Product verification was successful for FMID SSIB310V
Ready;
```

Figure 3-6. *Messages displayed during SnapShot Verification*

Step 15: Review Programmable Operator Considerations (Optional)

SIM Processing

In the VM environment, Service Information Messages (SIMs) are generated by an SVA subsystem for hardware exceptions and/or failures. It is recommended that an automated operations facility, such as the **PRogrammable OPerator facility (PROP)** or another third party package, be utilized to process these messages. SVAA provides a PROP action routine to handle SIMs that are unique to the SVA subsystem. The SVAA PROP action routine will identify the SVA subsystem and translate the SIM into a more descriptive message for operations.

SIM Installation

To process SVA SIMs, the installation's PROP userid must be able to execute the SIBADMIN command. To accomplish this, the PROP userid requires the following setup:

- 5MB minimum of virtual storage.
- Access to the SVAA RUN disk.
- PROFSIBA SVAA macro with all SVA subsystems identified via the SET ECAMDEVICE subcommand.

The SVAA sample library, SIBSAMP MACLIB (on the RUN disk), contains a sample PROP routing table member called RTABLE. This file has the following PROP routing table statements that enable SIBPROP to process SVA subsystem SIMs:

```
*----------------------- --- --- -- -------- -------- -------- --------
*T                       S   E   T  U        N        A        P
*E                       C   C   Y  S        O        C        A
*X                       O   O   P  E        D        T        R
*T                       L   L   E  R        E        N        M
*----------------------- --- --- -- -------- -------- -------- --------
* Trap SVA SIM alert messages.
*----------------------- --- --- -- -------- -------- -------- --------
/HCPERP403I/REFCODE=       10  29  3                   SIBPROP  REFCODE
/REFCODE=                  10  17  3                   SIBPROP  REFCODE
/HCPERP403I/               10  19  3                   SIBPROP  ALERTMSG
/SIB                        1   3  1                   SIBPROP  NOTIFY
```

If the installation is currently trapping SIM alert messages for other purposes, the SIBPROP EXEC may be modified to invoke other action routines in addition to the SVAA action routine that processes SVA SIMs.

Step 16: Define SVAA's DisContiguous Saved Segment (Optional)

It is highly recommended that a DisContiguous Saved Segment (DCSS) be defined for SVAA. There are many advantages to defining a DCSS. One of the advantages is the ability to share the virtual storage with other VM users executing the SVAA software and, thus, reduce the VM paging load. In addition, the SVAA software loads much faster. Finally, the DCSS can be defined outside the range of the VM user's defined virtual storage. At the very least, the small, .5MB, DCSS should be defined and will contain the routines that impact the most users.

Another option is to define two DCSS segments: a small and a large. The small one would contain the routines that impact the most users and is appropriate for general use. The large DCSS could be used by system programmers and storage administrators: users who are most likely to use SIBADMIN or SIBMENU. The disadvantage of defining two SVAA DCSS segments is the management involved with ensuring that the proper module is executed. On the other hand, defining two DCSS segments optimizes the performance of SVAA and virtual storage usage on the VM system.

SVAA's DCSS maintenance allows you to select a name for the saved segment, the beginning address of the segment, and one of three segment sizes: small (.5MB), medium (3MB), or large (6MB). The larger the segment the more SVAA code is included. The segment can exist above the 16MB line, but not all of the SVAA routines can be loaded above the line. If the segment is defined above the line, the few SVAA routines that have an RMODE 24 attribute are not included in the DCSS. At SVAA execution, those routines are loaded from the standard SVAA load module library.

You should avoid defining the SVAA DCSS with a segment address range that overlaps other segments that might be used while SVAA is active (e.g., CMS, ISPF).

To perform SVAA saved segment maintenance, the MAINTSTK userid requires authorization to execute the CP DEFSEG and SAVESEG commands. Normally these commands require privilege Class E. Virtual machine size must also be set above the ending address of the SVAA saved segment. Storage size may need to be adjusted to accommodate nucleus extensions and/or CMS storage allocations.

To define and save a single SVAA DCSS:

- Enter **NSSIB310** with no parameters. The EXEC prompts you for the name, size (small, medium, or large), and starting address of the saved segment.

To switch SVAA back to run without a DCSS,

- purge the DCSS. For example, enter:

  ```
  CP PURGE NSS SVAADCSS
  ```

- or run NSSIB310 and specify a new DCSS name but don't save it. If SVAA does not find a valid DCSS to use, it runs without the shared segment.

To define and save two SVAA DCSS segments, a small and a large:

1. Define a small segment by entering **NSSIB310** with no parameters. The EXEC prompts you for the name, size (small, medium, or large), and starting address of the saved segment. When prompted for the size of the segment, specify small.

2. Copy the following files from the SVAA RUN disk to another minidisk after the small segment has been defined:

```
SIBLLAPI    MODULE
SIBVMCUR    MODULE
SIBVMRVA    MODULE
```

   These modules contain the DCSS name.

3. Define the large DCSS segment by entering **NSSIB310** with no parameters. The EXEC prompts you for the name, size (small, medium, or large), and starting address of the saved segment. When prompted for the size of the segment, specify large.

To use the small DCSS, execute the module files copied to the minidisk in step 2 above. To use the large segment, execute the modules on the SVAA RUN disk.

Step 17: Apply Maintenance (Required)

Cumulative maintenance PTFs are initially distributed via a Maintenance tape. PTFs created after this Maintenance tape must be reinstalled as part of this procedure.

To apply maintenance from tape or download file:

1. Log onto the maintenance virtual machine (for example, MAINTSTK).
2. Back up the maintenance machine's MERGE and RUN disks.
3. Attach a tape drive as virtual device 181 (and continue to step 4), or download the cumulative maintenance file from the StorageTek Customer Resource Center site (www.support.storagetek.com) and go to step 7 (below).
4. Mount the Maintenance tape on the selected drive.
5. Load the maintenance memos onto the A-disk by entering:

   ```
   ACCESS 191 A
   VMFPLC2 REW
   VMFPLC2 LOAD * * A
   ```

6. Print the maintenance memos that are loaded from the tape.
7. Load the maintenance files onto the DELTA disk by entering:

   ```
   EXEC SSSIB310
   ```

   After the maintenance files are loaded onto the DELTA disk, the EXEC will prompt you to apply the PTFs.
8. If you had previously applied PTFs that are not part of this Maintenance, they must be applied again. Repeat the following steps for each product FMID PTF (e.g., SSIB310V, SSOC210V, SSNI210V, and SSKP124V).

   a. Apply other PTFs.

      ```
      VMFMERGE SSIB310V PTF ptfnum      (to apply a single PTF)
      VMFMERGE SSIB310V PTFLIST ptflist (to apply a list of PTFs)
      ```

   b. Apply any zaps.

      ```
      VMFZAP SSIB310V
      ```

9. To generate the run-time software, enter:

   ```
   EXEC GENSVAA
   ```

   This EXEC will, in turn, execute the generation EXECs for each FMID: GSSIB310, GSSNI210, GSSKP124, and GSSOC210.
10. If an SVAA DCSS is defined, you will need to save the DCSS again. Enter:

    ```
    EXEC NSSIB310
    ```

11. Detach virtual tape 181, if necessary. Enter:

    ```
    DET 181
    ```

Chapter 4. Customizing Your SVAA Installation

Customizing SVAA consists of the following tasks (which this chapter describes in detail):

Step 18 Customizing the ISPF main panel

Step 19 Customizing the default SVAA profile

Step 20 Customizing Reporter

Step 21 Customizing the SYSPROF EXEC

Step 18: Customizing the ISPF Primary Panel for SVAA Software (Optional)

You can access SVAA functions from ISPF panels. “Step 24: Using SVAA with SVA Subsystems (Required)” on page 5-4 describes how to display the SVAA Main Menu from CMS using the SIBMENU command.

This step describes how to add an SVAA selection to the ISPF Primary Panel (ISP@PRIM). (If you are using PDF, the panel is ISR@PRIM.)

To add SVAA to the ISPF Primary Panel:

1. Access, in read/write mode, the minidisk that contains the ISPPLIB MACLIB file.

   For PDF: access the ISRPLIB MACLIB file.

2. Enter **TERM CHARDEL OFF**

3. Use XEDIT with the MEMBER option to modify the ISP@PRIM member of the ISPPLIB MACLIB file. Add the highlighted lines in the example shown in Figure 4-1.

   For PDF: edit the ISR@PRIM member of the ISRPLIB MACLIB file.

4. Save the file.

5. Enter **TERM CHARDEL ON**

For more information about modifying the ISPPLIB MACLIB file, refer to the appropriate IBM documentation.

Note: The ISPF environment with SVAA requires a minimum of 5 megabytes of virtual storage. If you receive the VM message DMSMOD109S, you do not have enough virtual storage to run SVAA, and the amount of virtual storage should be increased.

```
%------------------------  SAMPLE PRIMARY OPTION MENU  -------------------------
%OPTION  ===>_ZCMD                                                             +
%                                                        +USERID   - &ZUSER
%   0 +ISPF PARMS  - Specify terminal and user parameters   +TIME     - &ZTIME
%   1 +COMMANDS    - Create/change command table            +TERMINAL - &ZTERM
%   2 +ISPPREP     - Preprocessed panel utility             +PF KEYS  - &ZKEYS
%   3 +ISPDTLC     - ISPF DTL Conversion Utility
%   4 +.           - (Description for option 4)
%   5 +.           - (Description for option 5)
%   7 +DIALOG TEST - Perform dialog testing
%   I +SVAA        - Shared Virtual Array Administrator
%   T +TUTORIAL    - Display information about this application
%   X +EXIT        - Terminate ISPF using list/log defaults
%
+Enter%END+command to terminate application.
%
+5684-043 (C) COPYRIGHT IBM CORP. 1980, 1990
)INIT
  .HELP = ISP00003      /* Help for this panel                    */
  &ZPRIM = YES          /* This is a primary option menu          */
  &ZHTOP = ISP00003     /* Tutorial table of contents for this appl*/
  &ZHINDEX = ISP91000   /* Tutorial index - 1st page for this appl */
  VPUT(ZHTOP,ZHINDEX) PROFILE
)PROC
  &ZSEL = TRANS( TRUNC (&ZCMD,'.')
                0,'PANEL(ISPOPTA)'
                1,'PANEL(ISPUCMA)'
                2,'PGM(ISPPREP) NEWAPPL'
                3,'CMD(%ISPDTLC)'
                7,'PGM(ISPYXDR) PARM(ISP) NOCHECK'
           /*********************************************************/
           /*                                                       */
           /* Add other applications here.                          */
           /*                                                       */
           /*********************************************************/
               I,'CMD(SIBREMM0) NOCHECK'
               T,'PGM(ISPTUTOR) PARM(ISP00000)'
             ' ','  '
               X,'EXIT'
               *,'?' )
  &ZTRAIL = .TRAIL
)END
```

Figure 4-1. *Sample ISPF primary panel (ISPPLIB MACLIB)*

Step 19: Customizing the Default SVAA Profile (Optional)

The MAINTSTK 454 minidisk contains the PROFSIBA SIB REXX macro, which is the default SVAA user profile for the command line interface to SVAA. Figure 4-2 shows a section of the default PROFSIBA SIB macro that you should customize.

```
/* */

**  Access SVA subsystem SYSA and SYSB for SVAA Communication.
*/
/*  call cpcmd "ERRMSG LINK $SUBSYS$ 200 200 MW"
**  call cpcmd "ERRMSG LINK $SUBSYS$ 210 210 MW"
**
**  "SET ECAMDEVICE (200 210)"
*/

/*
**  SVAA Device Mapping.
**  Caution - refer to the SVAA Device Mapping section
**            of the SVAA for VM Installation Guide for
**            behavior in non-contiguous device ranges.
*/

/*
**  "SET DEVICEMAP (ON)"
*/
*/
```

Figure 4-2. *Default PROFSIBA SIB macro*

In Figure 4-2, the commented lines (shown in bold type) contain the following sample statements:

- CP links to the minidisks that you defined in Step 8 on page 3-6.
- SET ECAMDEVICE statements that specify which ECAM devices you use for communications between SVAA and SVA.
- SET DEVICEMAP(ON) associate an SVA functional device with a host device address and volser. Device mapping is discussed in more detail in Step 8 on page 3-6.

For example, to use both SVA subsystems for which you defined ECAM devices, you could modify the sample as shown in Figure 4-3 on page 4-5.

```
/* */

/*
**  Access SVA subsystem SYSA and SYSB for SVAA communication.
*/

call cpcmd "ERRMSG LINK $SUBSYS$ 200 200 MW"
call cpcmd "ERRMSG LINK $SUBSYS$ 210 210 MW"
"SET ECAMDEVICE (200 210)"

/*
**  SVAA Device Mapping.
**  Caution - refer to the SVAA Device Mapping section
**            of the SVAA for VM Installation Guide for
**            behavior in non-contiguous device ranges.
*/

"SET DEVICEMAP (ON)"
```

Figure 4-3. *Modified PROFSIBA SIB macro*

You can also add SVAA subcommands to the sample macro. Refer to the *SVAA for VM Configuration and Administration* and *SVAA for VM Reporting* manuals for detailed information about SVAA subcommands.

Step 20: Customizing Reporter (Optional)

You can customize Reporter for your company's needs by completing some or all of the following tasks:

- Customizing the PROFILE EXEC for STKSRP
- Copying the sample macros
- Customizing PROFSIBS SIB
- Customizing SIBSRPAC SIB
- Initializing STKSRP

Step 20A: Customizing the PROFILE EXEC for STKSRP (Optional)

This step is optional depending on whether or not you want to use Reporter. In the PROFILE EXEC for STKSRP, you may want to spool the console to a maintenance user ID for audit and diagnostic control. Figure 4-4 shows a portion of a sample PROFILE EXEC. You may modify an existing PROFILE EXEC to add the lines shown in the figure, or you may create a new PROFILE EXEC. The line you may want to modify is shown in bold type.

```
/* */
  Trace Off

  Address Command

/*
**  Spool the console
*/
  'CP SPOOL CONS START TO * HOLD'
  Queue 'SIBSRP'
  Exit rc
```

Figure 4-4. *Sample PROFILE EXEC for STKSRP*

Note: SIBSRP is the program that collects the performance data.

Step 20B: Copying the Sample Macros (Optional)

Although this step is optional, it is required if you want to use Reporter. In Step 9 on page 3-10, you defined the STKSRP user ID and linked to the MAINTSTK 454 minidisk. In this step, you copy the sample SVAA macros to STKSRP's 191 (A) minidisk so you can customize these macros in Step 20C and Step 20D.

To copy the sample macros:

1. Log on to STKSRP.
2. If you did not link to MAINTSTK's 454 minidisk as STKSRP's 192 minidisk, use the CMS ACCESS command to access this minidisk as the "D" disk.
3. Copy the sample macros to the A minidisk. For example, enter the following commands:

```
COPY PROFSIBS SIB D = = A
COPY SIBSRPAC SIB D = = A
```

Step 20C: Customizing PROFSIBS SIB (Optional)

Although this step is optional, it is required if you want to use Reporter. You can use the PROFSIBS SIB macro to define the Reporter profile. Figure 4-5 on page 4-8 shows a portion of the sample PROFSIBS SIB file with the SVAA subcommands (shown in bold type) that you may want to modify described in the following list:

LINK statements
: Links to the ECAM and non-SVA devices that you defined in Step 8 on page 3-6.

SET ECAMDEVICE statements
: Specify the ECAM devices used for communication between SVAA and the SVA.

SET NONICEBERG
: Specifies the non-SVA devices used to communicate statistics to Reporter.

INITIALIZE MAINLOG
: Defines the files to be used for data collection.

COLLECT PTDATA
: Starts performance-tracking (PT) data collection.

SET DEVICEMAP(ON)
: When SET DEVICEMAP(ON) is invoked, diagnose I/O is performed to the ECAM devices to identify device characteristics. This process is called device mapping and its purpose is to associate an SVA functional device with a host device address and volser. Device mapping is discussed in more detail in the *SVAA for VM Configuration and Administration* manual.

```
/* */

/*
**  Access SVA subsystem SYSA and SYSB for SVAA communication.
*/

/*  call cpcmd "ERRMSG LINK $SUBSYS$ 200 200 MW"
**  call cpcmd "ERRMSG LINK $SUBSYS$ 210 210 MW"
**
**  "SET ECAMDEVICE (200 210)"
*/

/*
**  SVAA Device Mapping.
**  Caution - refer to the SVAA Device Mapping section
**            of the SVAA for VM Installation Guide for
**            behavior in non-contiguous device ranges.
*/

/*
**  "SET DEVICEMAP (ON)"
*/

/*
**  Access the minidisk used to record the performance data.
*/

    address COMMAND "ACCESS 196 B"

/*
**  Initialize the main logging file.
*/

    "INITIALIZE MAINLOG ( OUTFILE(&DAYDATE SRPDATA B) )"

/*
**  Initialize the data collection parameters.
*/

    "COLLECT PTDATA( INTERVAL(15M) SYNC(15M) )"
```

Figure 4-5. *Sample PROFSIBS SIB macro*

For example, to start data collection for both SVA subsystems and for the non-SVA devices for which you defined communications devices, you could modify the sample as shown in Figure 4-6 on page 4-9.

```
/* */

/*
**  Access SVA subsystem SYSA and SYSB for SVAA communication.
*/

call cpcmd "ERRMSG LINK $SUBSYS$ 200 200 MW"
call cpcmd "ERRMSG LINK $SUBSYS$ 210 210 MW"

"SET ECAMDEVICE (200 210)"

/*
**  SVAA Device Mapping.
**  Caution - refer to the SVAA Device Mapping section
**            of the SVAA for VM Installation Guide for
**            behavior in non-contiguous device ranges.
*/

"SET DEVICEMAP (ON)"

/*
**  Access the minidisk used to record the performance data.
*/

    address COMMAND "ACCESS 196 B"

/*
**  Initialize the main logging file.
*/

    "INITIALIZE MAINLOG ( OUTFILE(&DAYDATE SRPDATA B) )"

/*
**  Initialize the data collection parameters.
*/

    "COLLECT PTDATA( INTERVAL(15M) SYNC(15M) )"
```

Figure 4-6. *Modified PROFSIBS SIB macro*

You may also want to add SVAA subcommands to the PROFSIBS SIB file. See the *SVAA for VM Reporting* manual for details of SVAA Reporter subcommands.

Step 20D: Customizing SIBSRPAC SIB (Optional)

Although this step is optional, it is required if you want to use Reporter. Edit STKSRP's SIBSRPAC SIB file to authorize VM user IDs to execute Reporter subcommands. Figure 4-7 shows a portion of the sample SIBSRPAC SIB file with the line you may want to modify shown in bold type.

Enter the IDs of users you want to be authorized to execute Reporter subcommands in the following format:

"user1 user2 ..."

```
/* */

arg user command

/*
**  Check the list of authorized userids for the requesting userid.
*/
userid = "user1 user2 ..."   /* Place authorized userids inside quotes */
if find(userids,user) > 0 then rcValue = 0
                          else rcValue = 1

exit rcValue
```

Figure 4-7. *Sample SIBSRPAC SIB macro*

Step 20E: Initializing STKSRP (Optional)

This step is optional, whether or not you want to use Reporter. STKSRP runs as a disconnected service virtual machine. If you want STKSRP to be automatically logged on when VM is IPLed, you should add the following statement to your VM IPL procedures:

```
XAUTOLOG STKSRP
```

Step 21: Customizing the SYSPROF EXEC (Optional)

The SYSPROF EXEC is a system profile for CMS that is shipped as file SYSPROF $EXEC. To make any changes to it you should use the VMSES/E Local Modification procedure. Refer to the VM document CMS Planning and Administration for a complete section on "How to Change the SYSPROF EXEC".

NCL Management Using SIBVMCUR

In the CMS filesystem, a moving cursor (pointer) is used to allocate the next available block on a minidisk. In order to efficiently utilize physical space on an SVA, the moving cursor should always point to the lowest available block. In order to achieve this, SVAA provides a utility, SIBVMCUR, which sets the "low allocation" flag whenever the CMS ACCESS command is invoked for a R/W minidisk that resides on an SVA. In addition, a RELEASE option dynamically returns unused data tracks for minidisks residing on an SVA. It is highly recommended that SIBVMCUR be enabled for all users via the system's SYSPROF EXEC.

For more information regarding NCL Management and SIBVMCUR, see the *SVAA for VM Configuration and Administration* manual.

Instant Format Using a CMS FORMAT Intercept

SIBFMTSS is a replacement for the CMS FORMAT command for **SVA subsystems only**. It is recommended that SIBFMTSS be enabled for all users via the system's SYSPROF EXEC. CMS formats take time and use large amounts of system resources (CPU and I/O). However, by utilizing virtual technology, SIBFMTSS can perform the format almost instantaneously using minimal amounts of system resources. If SIBFMTSS determines that it is not possible to use "Instant Format," the normal CMS FORMAT command is performed.

Note: If the VM environment has a mixture of V2X series, V960, and earlier SVA subsystems, some additional parameters and preformatted disks will need to be defined. You should review details of the Instant Format feature, including special parameters, in the *SVAA for VM Configuration and Administration* guide.

Sample REXX Code to Enable SIBVMCUR and Instant Format

The following sample REXX code can be used to enable SIBVMCUR and Instant Format from the SYSPROF EXEC:

```
/*
**  Enable SVAA cursor reset and Instant Format for SVA minidisks.
*/

 Parse Value Diagrc('8', 'LINK MAINTSTK 454 1454 RR') With rc 10 .
 If rc = 0 Then
   Do
    'SET CMSTYPE HT'
    'ACCESS 1454 B'
    If rc = 0 Then
      Do
        'SIBVMCUR ON ( QUIET RELEASE'
        CALL SIBVMRVA
        'EXECLOAD SIBFMTSS EXEC B ( SYSTEM'
        If rc = 0 Then 'SIBTRAP FORMAT SIBFMTSS'
        'RELEASE B'
      End
    'SET CMSTYPE RT'
    Call Diag '8', 'DETACH 1454'
   End

EXIT
```

Figure 4-8. *Sample REXX code to enable SIBVMCUR and Instant Format*

The SVAA RUN disk files required to support SIBVMCUR and Instant Format are:

```
SIBFMTSS     EXEC
SIBLLAPI     MODULE
SIBNUCX      LOADLIB
SIBTRAP      MODULE
SIBVMCUR     MODULE
SIBVMRVA     MODULE
```

Chapter 5. Using SVAA

Using SVAA consists of the following tasks (which are detailed in this chapter):

Step 22 Establishing communications between SVAA and the SVA

Step 23 Changing the VM missing-interrupt handler (MIH) timeout value for DASD

Step 24 Using SVAA with SVA subsystems

Step 22: Establishing Communications Between SVAA and SVA (Required)

Your SVA hardware must be installed to complete this step. To establish communications between SVAA and the SVA subsystems, do the following:

- Define a privileged ECAM device at the SVA Local Operator Panel (LOP) or the Detached Operator Panel (DOP).
- Initialize the ECAM device.

Defining a Privileged ECAM Device

To define a privileged ECAM device, you complete a minimum system configuration at the LOP or the DOP. See the *V2Xf Shared Virtual Array: Operation and Recovery* manual for detailed instructions for completing this configuration.

During this configuration, use the Functional Device Configuration panel to create at least one functional device with the ECAM field set to `Y`. You may want to define two ECAM devices so that you will have a backup device available in case, for instance, you want to delete one of your ECAM devices.

Initializing ECAM Devices

In Step 8 on page 3-6, you defined minidisks that will map to the ECAM device(s) that you defined in "Defining a Privileged ECAM Device." Now you initialize an ECAM device by assigning a volume serial ID to one of the minidisks that you defined. Perform this procedure from the user ID that you use to initialize VM volumes.

To initialize an ECAM device:

1. Attach the device to the MAINTSTK user ID.
2. Run the ICKDSF utility to assign a volume serial ID to the device.

   Assign a volume serial ID that corresponds to a volume serial ID that you assigned to an ECAM device minidisk in Step 8 on page 3-6.
3. Detach the device from the MAINTSTK user ID.
4. Attach the device to the system.

Defining and Initializing SVA Devices

In the SIBSAMP MACLIB, SVAA provides a sample macro, SIBDEFDV, that defines and initializes SVA devices for VM use. This macro is documented within the sample file itself.

Step 23: Changing the VM Missing-Interrupt Handler Timeout Value (Required)

z/VM allows the Missing-Interrupt value to be dynamically set by the operating system based upon SVA device characteristics. The SVA returns the primary value for the DASD's missing interrupt handler, thus overriding the default of 15 seconds. The primary value is currently set to 5 minutes and 15 seconds, but this value may vary depending upon the SVA model. The setting may be verified by using the CP QUERY MITIME command.

Note: For prior releases of VM, you must change the default DASD MITIME for each SVA device by using the CP SET MITIME command For example, to set the MIH timeout value to 5 minutes and 15 seconds, execute the following CP command from a system startup exec or script:

```
CP SET MITIME rdev-rdev 05:15
```

where *rdev-rdev* is the range of the real device addresses that you have assigned to your SVA devices.

Step 24: Using SVAA with SVA Subsystems (Required)

You can now use SVAA to configure and report statistics for any SVA subsystems you defined. This section contains basic information for starting an SVAA session. See the *SVAA for VM Configuration and Administration* and *SVAA for VM Reporting* manuals for detailed instructions about using SVAA.

To use SVAA, you must have access to the the SVAA run-time software which resides on the MAINTSTK 454 minidisk if you used the example MAINTSTK definition in Step 7 on page 3-4. To link and access this minidisk, enter commands such as the following:

```
CP LINK MAINTSTK 454 198 RR
ACCESS 198 I
```

You can now access SVAA by two methods:

- SIBADMIN - the interactive SVAA command module
- ISPF panels

Accessing SVAA using SIBADMIN

To access SVAA using SIBADMIN, in CMS enter the following command:

```
SIBADMIN
```

Accessing SVAA through ISPF Panels

You can also access SVAA functions from ISPF panels. To display the SVAA Main Menu:

- If you modified the ISPF Primary Panel as described in Step 17 on page 3-21, select the SVAA option from this panel.
- If you did not modify the ISPF Primary Panel, in CMS enter the following command:

  ```
  SIBMENU
  ```

Appendix A. SIBSAMP MACLIB Files

The following is a list of SVAA VM sample entities with a description of each. Refer also to member ##DISCLM.

To extract these files to a CMS minidisk, use the SIBSAMPX command:

```
Format:  SIBSAMPX membername fn ft fm ( REPLACE
 where:  sampfn  = member name within the SIBSAMP MACLIB
         fn      = target file name. Default is "membername"
         ft      = target file type. Default is "MEMBER"
         fm      = target file mode. Default is "A"
         REPLace = replace the file if it exists
```

Member Name	Brief Description
LCMCONF	SnapVantage configuration file.
LCMCGI	SnapVantage Apache CGI scripts (binary).
LCMIMG	SnapVantage Apache bitmap images (binary).
LCMINST	SnapVantage installation EXEC.
LCMPROF1	SnapVantage PROFILE EXEC for the server userid.
LCMPROF2	SnapVantage PROFILE EXEC for the cloned userids.
LCMROOT	SnapVantage root scripts (binary).
RTABLE	Sample PROP routing table (RTABLE) with entries to trap SVA SIM alert messages.
SIBCEMSR	Sample SAS program (that invokes SAS/GRAPH) to produce the cache effectiveness monthly summary graph.
SIBDEFDV	SVAA Macro to define and initialize a functional device
SIBDPDSR	Sample SAS program (that invokes SAS/GRAPH) to produce the device performance daily summary graph.
SIBDPWSR	Sample SAS program (that invokes SAS/GRAPH) to produce the device performance weekly summary graph.
SIBNCL00	Configuration information and instructions for defining VM userids and installing the VM Interval NCL Management prototype.
SIBNCL01	Sample SVAA macro used to support the master service machine in the VM Interval NCL Management prototype.
SIBNCL02	Sample REXX EXEC used to support the slave service machines in the VM Interval NCL Management prototype.
SIBNCL03	Sample REXX EXEC used to control the console log for a VM Interval NCL Management prototype userid running disconnected.
SIBNCL04	Sample SIBMDSEL user exit to allow a user to exclude minidisks in the VM Interval NCL Management prototype.
SIBNCL05	Sample REXX EXEC to allow a user to LINK to a minidisk in the VM Interval NCL Management prototype.

SIBNCL06 Sample SVAA macro to release back-end storage for CMS minidisks that reside on an SVA.

SIBQMD01 Sample SVAA macro that invokes the QUERY MINIDISK subcommand against a list of VM minidisks and produces a report file.

SIBRUB01 Sample REXX EXEC that invokes the VM NCL minidisk rewrite utility, SIBRUB, for all accessed CMS disks in write mode.

SIBRUB02 Sample REXX EXEC that invokes the VM NCL minidisk rewrite utility, SIBRUB, against a list of CMS disks.

SIBSGR01 Sample SAS program (that invokes SAS/GRAPH) to produce the average service time and average transfer size graph from Data Extract output from Reporter.

SIBSGR02 Sample SAS program (that invokes SAS/GRAPH) to produce the average service time and cache hit percent graph from Data Extract output from Reporter.

SIBSGR03 Sample SAS program (that invokes SAS/GRAPH) to produce the average service time and data throughput graph from Data Extract output from Reporter.

SIBSGR04 Sample SAS program (that invokes SAS/GRAPH) to produce the average service time and I/O rate graph from Data Extract output from Reporter.

SIBSGR05 Sample SAS program (that invokes SAS/GRAPH) to produce the average service time graph for the twenty-five busiest functional devices from Data Extract output from Reporter.

SIBSGR06 Sample SAS program (that invokes SAS/GRAPH) to produce the I/O service time at maximum I/O rate graph from Data Extract output from Reporter.

SIBSGR07 Sample SAS program (that invokes SAS/GRAPH) to produce the SVA free space analysis graph from Data Extract output from Reporter.

SIBSRPSH Sample REXX EXEC that summarizes SRP raw data files and manages the SAS data files that are created with the SVAA SUMMARIZE HISTORYDATA subcommand.

SIBSUIR Sample SAS program (that invokes SAS/GRAPH) to produce the space utilization interval graph.

SIBSUMSR Sample SAS program (that invokes SAS/GRAPH) to produce the space utilization monthly summary report.

SIBXGR00 Sample Microsoft Excel macro to produce the recommended graphs from Data Extract output from Reporter. This is a *binary* file.

The SVAA SOCSAMP MACLIB contains the following files:

SOCVSS01 Sample REXX EXEC that uses the SNAP MINIDISK subcommand to duplicate a minidisk.

SOCVSS02 Sample REXX EXEC that uses the SIBVMRVA service utility to duplicate a minidisk.

Glossary

This glossary is included in each book in the Shared Virtual Array Administrator library. All of the terms are associated with SVAA, but not all are used in this specific document.

A

Alias. A pseudo-device used by the operating system to support an additional I/O path to a Base device. Each Alias device supports one additional I/O to a Base. See also: Base and Parallel Access Volume.

array. A group of storage devices that are used collectively to achieve data redundancy and/or improved performance. In the SVA, an array consists of either 7 or 15 drive modules. See also: dual-redundancy array.

array cylinder. The collection of all physical cylinders in a dual-redundancy array that have the same physical cylinder address (CC). The SVA allocates back-end space in units of array cylinders. There are two types of array cylinders: free and allocated.

array device. The disk devices that are logically grouped together when a FORM ARRAY command is issued at the local operator panel or from SVAA.

array track. The collection of all physical tracks in a dual-redundancy array that have the same physical track address (CC, HH).

B

back-end storage. The data storage portion of a storage subsystem. In the SVA, the disk arrays.

Base. A real device that supports additional I/O paths to itself in the form of Alias devices. Each Alias device supports one additional I/O to a Base. Multiple Alias devices can be associated with a single Base. See also: Alias and Parallel Access Volume.

base functional device ID (BFDID). The functional device identifier that maps to or from the lowest (base) interface address on a given channel.

C

cache. Solid state, random access memory that is located in a controller. The cache retains frequently used data for faster access by the channel. In the SVA, all data access is through cache.

cache fast write (CFW). A form of fast write in which data is written directly to cache storage without using nonvolatile storage and is available for later destaging.

channel end. The indication from the channel that it has completed an operation.

channel interface. The Disk Array Controller circuitry that attaches to the host channels.

cluster. See storage cluster.

collected free space %. The percentage of array cylinders that are free array cylinders (collected and completely free of user data).

compaction. The SVA process that eliminates inter-record gaps normally associated with CKD DASD. Compaction reduces the amount of wasted disk array space, thus reducing the net capacity load on the subsystem.

compression. The SVA process that reduces the size of data records by translating them to a different encoding scheme that requires fewer bytes of real storage.

controller. See Disk Array Controller.

count-key-data (CKD). A recording format that writes variable-length records. Each record consists of 1) a count field, which specifies the length of the (optional) key field and data field of the record, 2) the (optional) key field, and 3) a data field. The first record on each track contains a fourth field, home address.

current data. User data, stored in a disk array, that has valid pointers from internal SVA mapping tables.

D

DASD fast write (DFW). A form of fast write to cache in which data is written concurrently to cache and nonvolatile storage (NVS) and is subsequently scheduled for destaging to the disk arrays. Both copies are retained in the SVA Disk Array Controller until the data is completely written to the disk arrays.

Data Bridge. A pair of devices used by Power PPRC to transmit all tracks on all primary devices from the primary subsystem to the secondary subsystem. These devices are not used to store customer data.

Data Collection Virtual Machine. The disconnected service machine that periodically requests SVA performance data.

dedicated connection. In an Enterprise Systems Connection Director (ESCD), a connection between two ports that is not affected by information contained in link frames. This connection restricts these ports from communicating with any other port. The two ports have a dedicated connection that appears as one continuous link.

destage. The nonsynchronous write of new or updated data from the cache storage or nonvolatile storage to the Disk Array Units.

device. See (1) drive module and (2) functional device.

device end. An indication from an I/O device that it has ended an operation.

device reconstruction. The SVA automatic background function of recreating and rewriting all of the data that was stored on a failed device to a spare device using the functional track recovery process.

direct access storage device (DASD). A storage device in which the medium is always available to the read/write head without having to be mounted by an external agent.

disk array. The SVA's logical grouping of drive modules. See also: dual-redundancy disk array.

disk array capacity. The formatted physical capacity of a disk array excluding redundancy data.

Disk Array Controller. The SVA control unit that provides the interface intelligence between the host(s) and the back-end storage.

Disk Array Unit (DAU). A single physical frame containing drive modules that comprise the disk array storage in an SVA subsystem.

domain. See SCSI domain.

drain. The SVA process that gradually moves data stored on a device or a disk array to other devices. Drain operations allow for the nondisruptive deinstallation of a device or a Disk Array Unit.

drive module. A disk storage device consisting of the access arms and heads, disk surfaces, and the supporting electronics required to locate, write, and read data. Each drive module is physically packaged as a single field-replaceable unit (FRU) within the SVA.

drive reconstruction. See device reconstruction.

dual-redundancy disk array. A disk array that allows for real-time automatic recovery of data from up to two failed devices within the array.

In the V2X and V960 SVAs, a dual-redundancy disk array consists of 15 (13+2) drive modules. The array has a capacity equivalent to 13 drives of user data and 2 drives of redundancy data. (In the SVA, redundancy data is distributed among all 15 drives).

In the 9500 and earlier SVAs, arrays of 7 (5+2) drive modules can also be formed.

Dynamic Configuration. An SVA feature that allows the channel interfaces and up to 4096 functional volumes to be defined and/or altered. The functional configuration of an SVA subsystem can be determined by user requirements rather than available drive modules.

E

ECAM device. A functional device over which SVAA-based communication between the SVA Disk Array Controller and the host CPU(s) takes place.

ESCON channel. A channel that uses ESCON cables to transmit data between the host and the Disk Array Controller.

Extended Control and Monitoring (ECAM). The communications protocol that permits communication between SVAA and the SVA.

extent. A range of disk addresses expressed as a cylinder head range (CCHH) for a CKD device, or a logical block address (LBA) for a SCSI device.

F

fast write. A write operation that does not require immediate synchronous transfer of data to a DASD device, thus reducing the time an application must wait for channel end and device end for an I/O operation.

fault symptom code (FSC). An error code, generated by a control unit or subsystem, that points to the area or FRU most likely causing a problem.

fault tolerance. The capability of a subsystem to continue operating without interruption and/or intervention despite a failure within the subsystem (e.g., hardware, power, cooling). Fault tolerance is generally measured in relation to inherent reliability, availability, serviceability, and recoverability for the product.

FDID map. See functional device identifier mapping.

fence. The automatic or manual separation of a logical path or physical component from the remaining operating portion of the subsystem. The fencing process provides for continuous operation of the subsystem and allows for deferred nondisruptive

servicing of field-replaceable units (FRUs) via hot-plugging.

A logical barrier on a node or path that prevents the use of that node or path.

FICON channel. A channel that uses fiber connections to transmit data between the host and the Disk Array Controller.

field-replaceable unit (FRU). The smallest self-contained component that can be individually replaced during a service or repair action.

fixed block architecture (FBA). (Contrast with CKD) A recording format in which every track of the device is formatted with a fixed number of fixed-length records (generally called sectors), each of which contains an identifier (ID) field and a data field.

flexvolume. A 3380 or 3390 CKD volume defined with less than the maximum number of cylinders. The range of cylinders allowed depends on the device type.

free array cylinder. An array cylinder that contains no current or non-current user data.

free space collection (FSC). The automatic SVA background task that relocates data from fragmented array cylinders in order to collect free space into empty array cylinders. Free space collection maximizes the efficiency of array cylinder writes.

free space collection load. The average percentage of array cylinder space that must be relocated in order to create empty array cylinders in the SVA.

front end. The portion of the SVA Disk Array Controller data path that passes data between the channels and the cache.

functional. The term used to describe the SVA interface as viewed by the host, application, and users. This interface appears as a 3990-3 subsystem interface.

functional/allocated. The user-allocated portion of a functional volume's space; that is, minidisks as defined in the VM directory.

functional capacity. The data storage capacity that the host, application, and users view. Used in reference to the space available for storing data in (1) a single functional device, or (2) all defined functional devices in an SVA subsystem.

functional device. The volume image that the host operating system receives when the “Read Device Characteristics” CCW is issued.

functional device identifier (FDID). The identifier for a functional device as it is known to the SVA. FDIDs range from 0 to FFF (hexadecimal) or from 0 to 4095 (decimal).

functional free space. The unallocated/unused portion of a functional volume's space, as defined in the VM directory.

functional track. The equivalent of a 3380- or 3390-DASD track. A functional track record is stored on contiguous sectors in an allocated array cylinder.

functional track directory (FTD). The SVA internal mapping table that contains one entry for each functional track associated with the functional volumes currently defined by the user.

functional track recovery (FTR). The automatic SVA process of recovering data from a physical track that is unreadable due to a media defect or a failed device. The SVA accomplishes functional track recovery by reading and processing the user data and redundancy data at corresponding physical track locations on the remaining devices in the array.

functional volume. See functional device.

G

global spares. See spare devices.

L

large volume. A 3390-9 CKD volume defined with 32760 cylinders.

link address. An address assigned during initialization that identifies a channel or control unit so that the channel or control unit can send and receive frames, and perform I/O operations. See logical paths.

LLAPI. An ECAM device driver available to vendors which provides the ability to query an SVA subsystem and its devices as well as the ability to manipulate functional tracks.

logical array. A grouping of devices into an array. The grouping of devices does not depend on their physical location.

logical partition. The subset of a processor unit that is allocated to support the operation of a systems control program.

logical paths. The relationship between a channel and a control unit that designates the physical path to be used for device-level communication between the channel and the control unit. This relationship is defined within the channel and control unit by a link address assigned to the control unit and a link address assigned to the channel.

M

MAINTSTK virtual machine. The virtual machine from which all maintenance for all SVA VM software products is performed.

MAT partition. The SVA partition consisting of drive modules that are not yet available for storing user data. Drive modules are automatically members of the MAT partition when they are first physically inserted in the SVA or when they have been drained of data.

Media Acceptance Test partition. See MAT partition.

N

net capacity load (NCL). This number is two KB times the number of physical sectors actually used to store user data, not including redundancy data. NCL is a percentage of the total number of sectors that are storing user data and is based on physical capacity used.

nonquiesced snap. A snap taken when the system is in full read-write access mode.

nonvolatile storage (NVS). The redundant solid state memory in the Disk Array Controller that remains active when ac power is removed. NVS protects any data that has not been written to the disk arrays.

P

Parallel Access Volume. A combination of a real device (Base) and one or more pseudo-devices (Aliases) that together support multiple concurrent I/Os to enhance performance.

parallel channel. A channel that uses bus-and-tag cables to transmit data between the host and the Disk Array Controller.

partition. The logical separation of devices, arrays, or groups of arrays to allow different modes of operation. The SVA supports a MAT partition, a Test partition, a Production partition, a Spares partition, and an Unavailable partition.

Note: The Test partition is not available in the V2X, V960, or 9500 SVA.

PAV. See Parallel Access Volume.

physical capacity. The physical space contained in (1) a single drive module, (2) a partition, or (3) an SVA subsystem.

physical device. See drive module.

privileged ECAM device. Privileged ECAM devices are the only devices that SVAA can use to send messages to the subsystem to request a change in the SVA's state. Such messages include those that alter the subsystem configuration or start a drain.

At least one privileged ECAM device must be defined in each SVA; all functional volumes in an SVA subsystem can be defined as privileged ECAM devices.

Production partition. The SVA partition consisting of drive modules assigned to production arrays for storing user data.

PROFSIBA macro. The profile executed when the SVAA SIBADMIN program is started.

PROFSIBS macro. The profile executed when the SVAA Subsystem Reporting Program is started.

Q

quiesce. To end a process by allowing operations to complete normally.

quiesced snap. A snap taken while the system is quiesced; all buffered transactions are flushed to disk storage.

R

read hit. The situation in which data requested by the read operation is located in cache.

read miss. The situation in which data requested by the read operation is not located in cache.

reconstruction. See device reconstruction

redundancy group. A logical grouping of devices that are protected from data loss due to a device failure by the use of redundancy (parity) data that is stored across the devices. Arrays in the SVA are redundancy groups that protect data against two simultaneous device failures. See also: dual-redundancy disk array.

Reporter. The SVAA subsystem reporting program—the SVAA component that collects subsystem performance data and produces reports based on that data, as well as on space utilization.

S

SCSI channel. See SCSI I/O interface.

SCSI domain. An SVA addressing scheme, prefixed to SCSI target and LUN addresses, that extends the number of addressable volumes from SCSI-attached host systems.

serial channel. A channel that uses fiber-optic (ESCON) cables to transmit data between the host and the Disk Array Controller. See also: ESCON channel.

Service Information Message (SIM). A message generated by the host processor upon receipt of sense information from the SVA that contains notification of a need for repair or customer action, or status information.

Shared Virtual Array (SVA). StorageTek's online, random access disk array storage subsystem composed of a Disk Array Controller and 16 to 64 disk drive modules.

Shared Virtual Array Administrator (SVAA). StorageTek's host software product that enables implementation of the extended storage management facilities of the SVA, and offers additional functions including SnapShot, NCL management, and reporting capabilities.

SIBADMIN module. The module used to invoke SVAA in command mode.

SIBLLAPI. An ECAM device driver available to vendors which provides the ability to query an SVA subsystem and its devices as well as the ability to manipulate functional tracks.

SIBMENU exec. The module used to invoke SVAA in menu mode.

SIBSRP module. The SVAA module for the subsystem reporting program.

SIBSRPAC exit. The user exit that authorizes a user to communicate with the SRP service machine via IUCV.

SIM alert. An operator console message that alerts the operator that an action requiring attention has occurred.

slot. The physical location of an SVA subsystem drive module.

snap. (noun) A duplication of a source volume or minidisk with SnapShot (see SnapShot). A snap is also the result of a successful SnapShot operation (not the use of a data mover). Synonymous with SnapShot. Contrast with *data mover copy*.

snap. (verb) To duplicate a functional volume or minidisk with SnapShot.

SnapShot. StorageTek's high-speed data-duplication facility, available only with the SVA and packaged with SVAA. SnapShot achieves great time-savings in duplicating volumes or minidisks because it only creates a second set of pointers to the data. No additional physical disk space is used in the process.

source. The minidisk or volume from which data is snapped.

spare devices. SVA drive modules that are physically installed but not logically associated with an array. Spare devices are used by the SVA to form new arrays or to automatically reconstruct and logically replace failed devices.

spares. See spare devices.

Spares partition. The SVA partition consisting of all of the spare devices in the subsystem. See spare devices.

SSID. See subsystem identifier (SSID)

Status Bridge. A pair of devices used by Power PPRC to transmit acknowledgements that the data was received at the other end. These devices are not used to store customer data.

storage cluster. A power and service region that processes channel commands and controls the data storage devices. The SVA contains two storage clusters, each of which contains interfaces for up to 16 channels.

subsystem free space. Storage space in the disk arrays that does not contain user data.

subsystem identifier (SSID). The identifier for a 3990 controller emulated within the SVA. From one to sixteen SSIDs (logical 3990s) can be defined in each subsystem. Within an installation, each logical 3990 is defined by a unique four-digit (hexadecimal) SSID.

subsystem reporting program (SRP). The SVAA component that collects subsystem performance data and produces reports based on that data, as well as on space utilization. See also: Reporter.

SVAA profile facility. When invoked, this facility allows the user to specify commands for an SVAA session.

T

target. The minidisk or volume to which data is snapped.

Test partition. The SVA partition consisting of drive modules assigned to a test array and containing test data. The Test partition allows user-controlled, host-driven, testing of arrays, as though they were production arrays.

Note: The Test partition is not available in the V2X, V960, or 9500 SVA.

tray. The physical packaging of eight drive modules within the disk array area of the SVA.

U

Unavailable partition. The SVA partition consisting of drive modules that are not available for use in an array. Drive modules that are not installed or have failed are in this partition.

unit. See Disk Array Unit.

V

virtual device identifier (VDID). Another term for FDID. See functional device identifier (FDID).

volatile memory. See cache volatile memory.

volume. See functional volume.

volume serial number. A six-character alphanumeric name that identifies a disk volume to the host operating system.

W

write hit. The situation in which data to be updated by a write operation is located in cache.

write miss. The situation in which data to be updated by a write operation is not located in cache.

Abbreviations and Acronyms

API	application programming interface
BFDID	base functional device ID
CCHH	cylinder-head address (CC is the two-byte cylinder number, HH is the two-byte head number
CCW	channel command word
CFW	cache fast write
CKD	count-key-data
CLI	command line interface
CMS	Conversational Monitor System
CSI	consolidated software inventory
DASD	direct access storage device
DAU	Disk Array Unit
DFW	DASD fast write
DOP	Detached Operator Panel
DSF	Data Support Facilities
DTL	domain-target-LUN
ECAM	Extended Control and Monitoring
ESA	Enterprise Systems Architecture
ESCON	Enterprise Systems CONnection
ESDI	enhanced small device interface
FDID	functional device identifier
FICON	FIbre CONnection
FMID	function modification identifier
FRU	field-replaceable unit
FSC	fault symptom code, or free space collection
FTD	functional track directory
FTR	functional track recovery
GB	gigabyte
HCD	hardware configuration definition
ICKDSF	ICK Data Support Facilities
IDID	interface device identifier
IML	initial microprogram/microcode load
IOCP	I/O configuration program
IPL	initial program load
ISPF	Interactive System Productivity Facility
I/O	input/output
LBA	logical block address
LOP	Local Operator Panel
LUN	logical unit number
MAT	Media Acceptance Test
MB	megabyte
MIH	missing interrupt handler
MVS	Multiple Virtual Storage
NCL	net capacity load
NVS	nonvolatile storage
PAV	Parallel Access Volume
PPRC	peer-to-peer remote copy
PTF	program temporary fix
RACF	Resource Access Control Facility
RAID	redundant array of inexpensive disks
REXX	Restructured Extended Executor
RFA	record format assist
SAF	Security Access Facility
SCP	system control program
SCSI	small computer system interface
SIM	service information message
SMF	system management facility
SRP	Subsystem Reporting Program
SSID	subsystem identifier
SVA	Shared Virtual Array
SVAA	Shared Virtual Array Administrator
VCU	virtual control unit
VDID	virtual device identifier
VM	Virtual Machine
VM/ESA	Virtual Machine/Enterprise Systems Architecture
volser	volume serial number

Index

Special Characters

C

D

E

G

I

M

N

P

R

S

V

Reader's Comment Form

Product Name: Shared Virtual Array Administrator for VM
Manual Name: Installation, Customization, and Maintenance

Software Level: Version 3.1
Document Number: 313463107

Please check or fill in the items, adding explanations or comments in the spaces provided.

Which of the following terms best describes your job?

_ Field Engineer	_ Manager	_ Programmer	_ Systems Analyst
_ Engineer	_ Mathematician	_ Sales Representative	_ Systems Engineer
_ Instructor	_ Operator	_ Student/Trainee	_ Other (explain below)

How did you use this publication?

_ Introductory text _ Reference manual _ Student/Trainee _ Instructor text
_ Other (explain) _____

Did you find the material easy to read and understand?	_ Yes	_ No	(explain below)
Did you find the material organized for convenient use?	_ Yes	_ No	(explain below)

Specific criticisms (explain below):

Clarifications on pages _____

Additions on pages _____

Deletions of pages _____

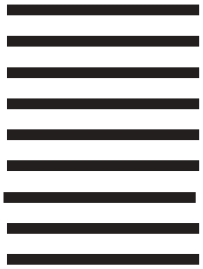
Errors on pages _____

Explanations and other comments:

Note: *Staples can cause problems with automated-mail sorting equipment. Please use pressure-sensitive tape to seal this form. If you would like a reply, please supply your name and address on the reverse side of this form. Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A.*

TO COMPLY WITH POSTAL REGULATIONS, FOLD EXACTLY ON DOTTED LINES AND TAPE (DO NOT STAPLE)

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 2 LOUISVILLE, CO U.S.A.

POSTAGE WILL BE PAID BY ADDRESSEE

STORAGE TECHNOLOGY CORPORATION
MANAGER, DISK STORAGE LEARNING PRODUCTS
ONE STORAGETEK DRIVE
LOUISVILLE, COLORADO 80028-2121
U.S.A.

FOLD HERE AND TAPE DO NOT STAPLE FOLD HERE AND TAPE

If you would like a reply, please print:

Your Name: _____

Company Name: _____ Department: _____

Street Address: _____

_____

Cut or Fold Along Line

Printed in U.S.A.

NEED MORE INFORMATION?

www.storagetek.com

ABOUT STORAGETEK

Storage Technology Corporation (NYSE: STK) is a $2 billion global company that enables businesses, through its information lifecycle management strategy, to align the cost of storage with the value of information. The company's innovative storage solutions manage the complexity and growth of information, lower costs, improve efficiency and protect investments. For more information, visit www.storagetek.com, or call 1.800.275.4785 or 01.303.673.2800.

WORLD HEADQUARTERS

Storage Technology Corporation
One StorageTek Drive
Louisville, Colorado 80028 USA
1.800.678.4430 or 01.303.673.4430

StorageTek equipment is manufactured from new parts, or new and used parts. In some cases, StorageTek equipment may not be new and may have been previously installed. Regardless, StorageTek's standard warranty terms apply, unless the equipment is specifically identified by StorageTek as "used" or "refurbished."

Replacement parts provided under warranty or any service offering may be either new or equivalent-to-new, at StorageTek's option. Specifications/features may change without notice.