Bull

SAN Manager
User's Guide

AIX

ORDER REFERENCE
86 A2 86KX 05

Bull

SAN Manager
User's Guide

AIX

Software

April 2001

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

ORDER REFERENCE
86 A2 86KX 05

Printed in France

Suggestions and criticisms concerning the form, content, and presentation of this book are invited. A form is provided at the end of this book for this purpose.

To order additional copies of this book or other Bull Technical Publications, you are invited to use the Ordering Form also provided at the end of this book.

Trademarks and Acknowledgements

We acknowledge the right of proprietors of trademarks mentioned in this book.

AIX® is a registered trademark of International Business Machines Corporation, and is being used under licence.

UNIX is a registered trademark in the United States of America and other countries licensed exclusively through the Open Group.

About This Book

This manual will help you to install and use the SAN Manager components and the NT software involved in the application.

Who Should Use This Book

It is written for the administrator who is to manage the SAN infrastructure components.

Overview

The manual is organized as follows:

- Introduction.
- SAN Manager Installation.
- Configuration file.
- Running SAN Manager Application.
- SAN Manager GUI.
- Monitoring Overview.
- SAN Administration Guidelines.
- Commands.
- SAN Manager Configuration and TCP/IP Configuration.
- Example of Using SAN Manager.
- Reporting Procedure on a Windows NT SAN Agent

Related Publications

- *AIX and Related Products Documentation Overview,* 86 A2 71WE.
- *Navisphere for AIX Setup and Operation,* 86 A1 47KX.
- *SYMMETRIX Storage Systems Reference Guide,* 86 A1 85KX.
- PowerConsole & Cluster Assistant Setup Guide, 86 A2 81HX.

Table of Contents

Chapter 1. Introduction

SAN Overview

A Storage Area Network, or SAN, is a high–speed network based on Fibre Channel technology. This 1 Gb/s data transfer interface maps several transport protocols including IP and SCSI, and hence allows you to merge high–speed I/O and networking functionality in a single connectivity technology. The SAN connects servers and large storage subsystems, and therefore is mostly dedicated to high–speed data transfers between these servers and the storage units.

SANs enable storage points to be distributed around the network at the level of the company site. Servers can then access storage peripherals several hundred meters away with response times comparable to local, private connections.

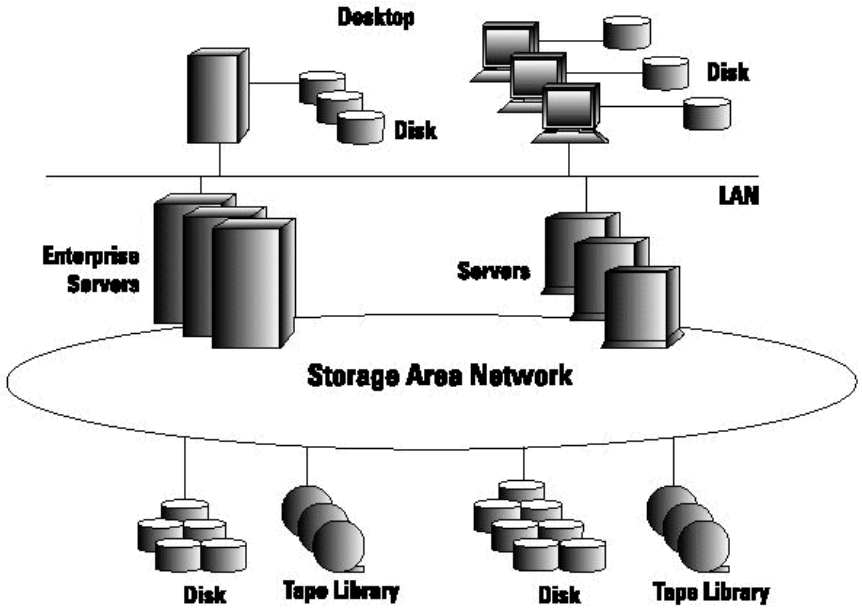


Figure 1. SAN overview

SAN Advantages

Obviously, SAN adds several major improvements to previous storage management strategies. Among these are:

- Distributed storage resources: any host on the SAN may view and access any storage system on the network.
- Scalability: new storage resources or new servers may be easily added onto the SAN; each server may increase its own storage resources at any time.
- Performance: Fibre Channel switches allow for modular increases in bandwidth. If the nominal speed of a Fibre Channel link is 1 Gbs, hundreds of independant data paths can be installed on a SAN, leading to almost unlimited bandwidth.
- Integrity and Availability: access paths to storage peripherals can be easily multiplied and the storage space allocated to each application server connected to the SAN can be duplicated. Gateways provide communication with remote SANs, opening the way for complete disaster protection solutions.

SAN Management needs

Increasing the size and complexity of these SAN networks raises new problems. In order to keep control over the whole SAN, an administrator will need to:

- visualize the available resources, as well as the network topology (which may increase in complexity as the networks develop),
- control the allocation of storage resources to servers (AIX or Windows NT) and prevent unauthorized access to data,
- restrict host visibility to necessary resources (to save boot time and to simplify administration),
- have a global view of the operational state of the various devices and correct the potential problems, rather than calling different management tools for all subsystems,
- have error logging for automated survey.

SAN Manager software has been developed by Bull to address all of these needs.

SAN Manager Presentation

Bull's SAN Manager for servers enables storage administrators to work more efficiently. It is built on a Web–based user interface. It means that browsing SAN storage resources becomes as simple as browsing a file system.

The SAN Manager greatly simplifies the management task by providing:

- Server–centric view of SAN infrastructures and disk subsystems,
- Graphical display of SAN Topology, with automatic refresh of the display whenever configuration changes occur (new components added, component status changed),
- Consolidation of information between other management tools: AIX, Open Symmetrix Manager, Navisphere for DAS,
- Centralization of event monitoring (faults detected on disk subsystems and switches are reported in SAN Manager
- Host–based LUNs Access Control to hide unauthorized resources to AIX and Windows NT servers.

Amongst other advantages, SAN Manager:

- is ideal for storage consolidation (no need to see resources used by other servers), in heterogeneous environment (AIX and Windows NT servers)
- makes EMC/Timefinder usable,
- enforces data confidentiality policies,
- reduces risk of administrator errors.

SAN Manager Architecture

The SAN Manager application comprises three functional parts:

- SAN agents that discover information about SAN components and perform actions on the hosts and subsystems: SAN agents exist for both AIX and Windows NT systems,
- client managers that are responsible for the end user interface and used in the WebSM server (AIX platforms only),
- a central agent that gathers information from SAN agents and answers requests from client managers (AIX platforms only).

The different parts of the SAN Manager application communicate with each other using TCP/IP, and they can be distributed between several machines:

- there must be only one instance of the *central agent* (AIX host only),

- there may be several instances of *client manager* (AIX host only),
- there should be one instance of the *SAN agent* per machine (AIX or Windows NT host) connected to the SAN.

But a single machine may contain several parts of the application (ie the same AIX platform can run both a *central agent* and a *client manager* or any other combination).

Each part of the application may comprise several processes; some of them are daemons that need to be started explicitly : on AIX hosts, this is the aim of the command ***/etc/rc.sanmgt start*** . This command uses a configuration file *(/etc/san/SANManager.cfg*) to know which part(s) of the application are to be started on the machine where /etc/rc.sanmgt is run (see SAN Manager Configuration File: SANManager.cfg, on page 3-1 for a description of this file).

On Windows NT hosts, the processes are started by the “S@N .IT!Scheduler” service using the SANManager.cfg file in the default installation directory (see SAN Manager Configuration File: SANManager.cfg, on page 3-1 for a description of this file).

Therefore the administrator must configure each of the machines involved in the SAN Manager application (by modifying the *SANManager.cfg* file on this machine) to describe:

- what are its role(s) in the SAN Manager application (central agent, client manager or SAN agent),
- if it has the client manager role or SAN agent role, where is the central agent.

As SAN agents and client managers declare themselves dynamically to the central agent, it is not necessary to stop the whole application to add new machines.

Refer to SAN Manager Configuration and TCP/IP Configuration, on page A-1 for a description of the SAN Manager application configuration versus TCP/IP.

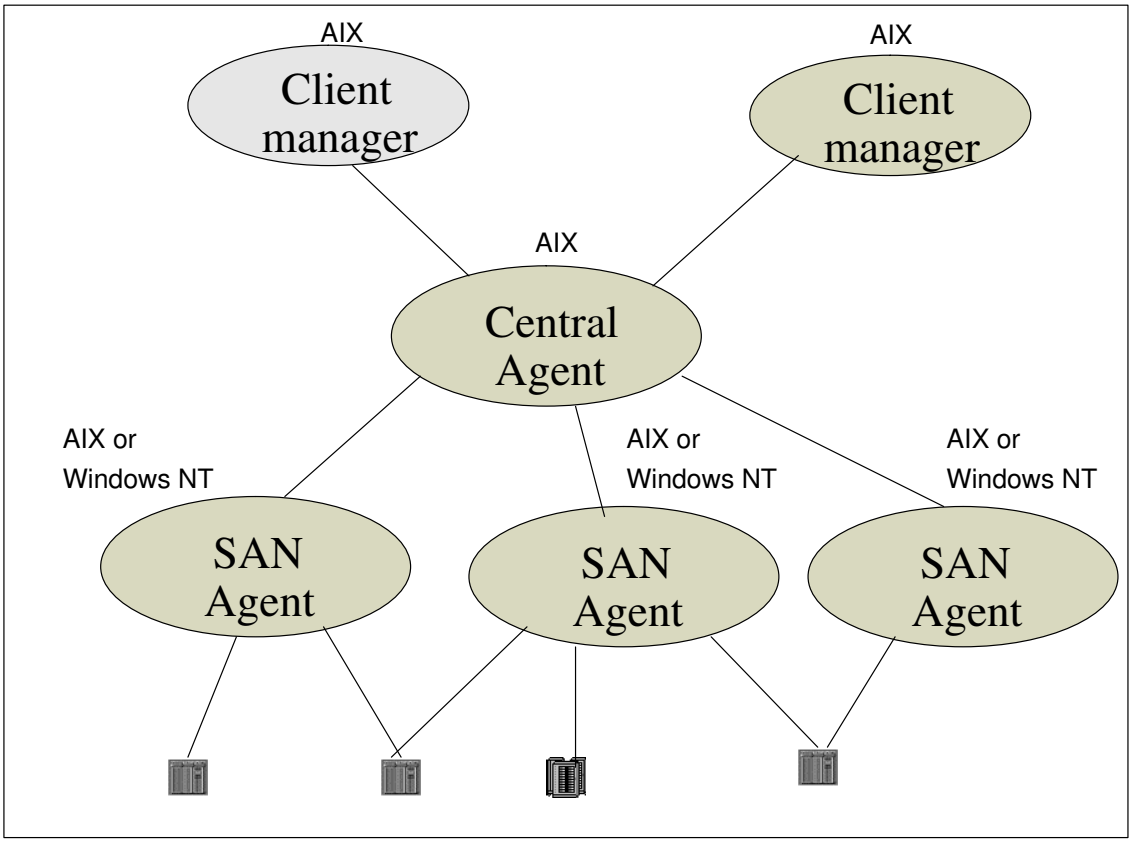


Figure 2. SAN Manager Architecture

SAN Topology

SAN interconnects:

- PCI–based AIX hosts with Emulex Fibre Channel adapters and Bull Fibre Channel driver.
- Windows NT hosts with Emulex LP8000 Fibre Channel adapters.
- Clariion DAS disk subsystems (including DAS 3500, DAS 5700, DAS 5720, DAS 5300, DAS 4500),
- EMC2 Symmetrix disk subsystems.

There are three different ways to interconnect SAN devices (with copper or fiber optic cables):

- with a single cable, which creates a point–to–point connection between two devices (a server and a dedicated storage system, for instance),
- to a hub, which creates a loop topology (called private loop), allowing communication between all the devices connected to the hub in circular fashion (as in Token Ring for instance),
- to a switch, which allows the creation of direct communication links between all pairs of devices connected to it.

These 3 types of connections are supported by SAN Manager.

Moreover, switches may be connected to other switches: this considerably increases the number of potentially connected devices, and still allows the creation of communication paths between any pair of devices. Such a communication network is called a fabric. Interconnection of switches to hubs is not allowed, but a fabric may be composed of several interconnected switches.

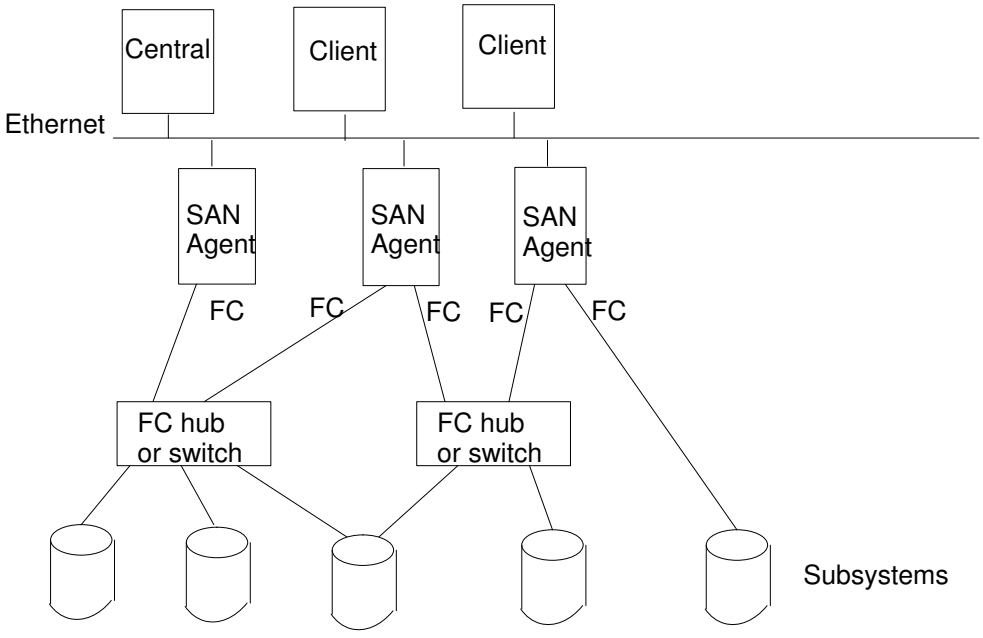


Figure 3. Typical topology of the SAN Manager.

View of SAN Devices

SAN disk devices are handled by AIX or Windows NT as any SCSI devices, and hence associated to AIX hdisks (or NT LUNs). But a major difference with local SCSI devices is that SAN networks allow you to define several (redundant) communication paths between a host and a given disk subsystem.

Hence, each SAN disk device may be associated with several AIX hdisk devices which may prove difficult to handle if the SAN integrates a large number of disk subsystems. See Managing multiple access paths to a subsystem, on page 7-2.

This forces the SAN Manager application to :

- give a better, LUN–consolidated view,
- handle the AIX hdisks (or NT LUNs) in a transparent way,
- reduce, with the LUNs Access Control, the total number of AIX hdisks (or NT LUNs) handled by the system to those which are really needed. This also saves boot time, which may prove of high interest if the SAN is very large.

LUNs Access Control

All hosts connected to a given fabric or private loop share the same visibility and access to the Logical UNits (or LUNs) of the disk subsystems on the same fabric or loop. This is what SAN Manager will show you when it is first launched.

Such permissiveness is not possible in an operational network: this is why SAN Manager provides you with a LUNs Access Control mechanism that allows you to decide, for each host, which LUNs will be accessible, and which won't.

LUNs Access Control information is centralized, and each host knows if other hosts have been allowed access to the same LUNs. Hence coherency control, which is the administrator's responsibility is easier.

LUNs will normally not be shared between hosts (except in very specific cases such as HA–configurations, for instance). It is very important to decide from the beginning to which LUNs access must be allowed, and to deny access to all other LUNs. Once LUNs Access Control is active, it is always possible to modify these access rights (i.e. allow access to an additional LUN, for instance).

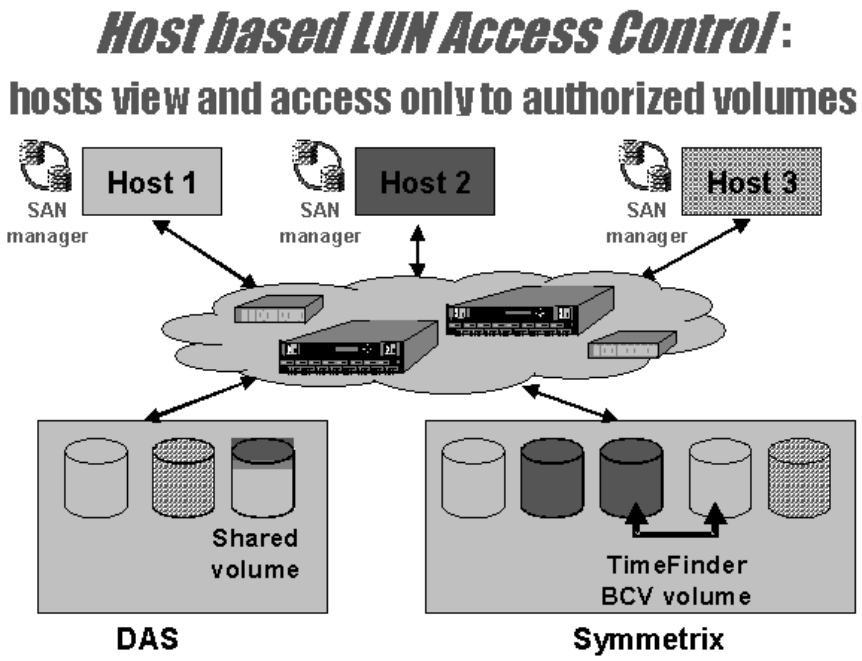


Figure 4. LUNs Access Control

Managing Multiple Paths to LUNs

A SAN allows for several paths between a host and a given disk subsystem.

Although very attractive for a network architect, such configurations should be handled with care.

Multiple access configurations should be built only with a specific purpose:

- to offer continuity of service in the case of hardware failure (connections via two different hubs or switches for instance),
- to increase total bandwidth (two connections between a subsystem and a given switch, for instance).

In such a configuration, each LUN of the subsystem will be associated to several hdisk devices on the AIX system (one disk for each path), and NT LUNs on the NT system.

These hdisk devices should not be used concurrently, except by appropriate software:

- you may for instance install ATF or PowerPath which will handle these devices, and make them visible to the end–user as a single device per each LUN,
- or you should use LUNs Access Control to keep only one hdisk (i.e. one path) per LUN.

Monitoring Subsystems and Switches

Subsystems and switches may be monitored via proprietary software (Navisphere for DAS, Symmetrix Management for EMC Symmetrix, Brocade SNMP agent tool for Brocade switches).

If this software is installed and correctly configured, monitoring information may be gathered and consolidated at SAN Manager level application.

Without monitoring, SAN Manager can only detect if a subsystem is accessible or unaccessible, not if it is operating correctly.

When a subsystem is monitored, SAN Manager indicates if an error has been detected and when it has been corrected.

For more information, refer to Monitoring, on page 6-1.

Domains

A domain is a group of hosts which share SAN resources.

Defining domains allows you to limit your display to the domain–visible part of the SAN topology, as seen from the hosts constituting the selected domain.

By default, there is only one domain, named domainAll, containing all the hosts connected to the SAN.

You may then create other domains, add or remove a host from a given domain, delete empty domains.

You may define as many different domains as you want: their definitions will be saved.

They have no effect on SAN Manager: you simply select a domain when you run the SAN Graphical User Interface (GUI) to define your own view of the SAN. It does not affect other user's visibility of the SAN.

Chapter 2. SAN Manager Installation

SAN Manager Installation Overview

The ”SAN Manager” is to be installed on all AIX servers that are involved in the application. The Windows NT SAN agent is to be installed on all Windows NT servers that are involved in the application.

The SAN Manager application is delivered on SAN Manager CD–ROM that contains both:

- the software to be installed on AIX servers,
- the software to be installed on Windows NT servers

The LUNs Access Control is initially created empty and is:

- ”inactive”. on AIX servers until the LUNs Access Control is activated, see page 5-15, the system continues to work as before, and all the LUNs remain visible.
- ”active”. on Windows NT servers until LUNs are made allowed for access by these servers, they cannot access the subsystem disks.

Installation of SAN Manager on AIX Servers

AIX 4.3.2 or later version is required.

The installation is managed through the SMIT interface and is completely automatic.

SAN Manager initial installation does not modify AIX behaviour, nor disk devices. It is transparent for ordinary users, and does not require a reboot.

Delivery

The ”SAN Manager” is delivered as a unique LPP (SANmgt) that contains 4 filesets:

- SANmgt.Common: pre–requisite for all other filesets,
- SANmgt.Client: part of application used by client manager,
- SANmgt.CentralServer: part of application used by the central agent,
- SANmgt.LocalServer: part of application used by the AIX SAN agents.

The software is delivered in the SAN Manager CD–ROM.

All filesets can be installed on all machines whatever the roles they will play in the application. These roles are determined by the configuration file. See SAN Manager Configuration File: /etc/san/SANManager.cfg, on page 3-1.

Prerequisites

The LPP prerequisites are:

- WebSM97 filesets for a client host.
- Java filesets.
- Netscape Web browser.
- Fibre Channel drivers for an AIX SAN agent.
  - devices.pci.df1001f7
  - devices.pci.df1001f8
  - devices.pci.df10e51a

In order to manage the disk subsystems, additional software may be required and installed at any time (before or after SAN Manager installation).

- Navisphere LPPs, and possibly ATF LPP, for DAS subsystems,
- Symmetrix Management packages, and possibly PowerPath LPP, for the EMC2 Symmetrix subsystems.

Installing Software on AIX servers

From the shell (or **dtterm** window), login as **root**.

Start SMIT by typing:

Fastpath = `smit [-C] install_latest` or `smitty install_latest`

`smit`	launches graphic mode
`smit -C`	launches ASCII mode
`smitty`	launches ASCII mode

From "`System Management`" menu, select the following sequence of sub-menus:

"`Software Installation and Maintenance`"

"`Install / Update Software`"

"`Install and Update from LATEST Available Software`"

A window opens. Select Input device = */dev/cd0*

`INPUT device / directory for software`

A window opens with a list of installation parameters:

`INPUT device / directory for software`	*/dev/cd0*
`SOFTWARE to install:`	`all_latest`
`PREVIEW only? (install operat. will NOT occur)`	`no`
`COMMIT software updates?`	`yes`
`SAVE replaced files?`	`no`
`AUTOMATICALLY install requisite software?`	`yes`
`EXTEND file systems if space needed`	`yes`
`OVERWRITE same or newer versions?`	`no`
`VERIFY install and check file sizes?`	**`yes`** (Note: default = no)
`Include corresponding LANGUAGE filesets?`	`yes`
`Detailed output?` (Note: this sets "verbose mode" for detailed audit log.	**`yes`** Default = no)
`Process multiple volumes?`	`yes`

To choose the software to install, click on F4.

Validate.

Confirm the message "`Are you sure?`"

The installation sequence is completed automatically with the progressive creation of the installation log, visible on the local monitor screen.

This installation log includes the following:

- list of all installed files and directory paths
- the text of the License Agreement
- preliminary installation check confirmation

- installation summary, showing for each installed software:
  - Name (Product Name)
  - Revision Level (n.n.n.n.), where **n** represents any number
  - User (User or Root)
  - Event (Application)
  - Result (Success).

A trace of this installation is saved in a dated log filed under */smit.log.*

/etc/san/SANManager.cfg

- During a first installation of SAN Manager, the `/etc/san/SANManager.cfg` configuration file is installed.

  It is necessary to configure this file after installation

- For an update or re–installation of SAN Manager, the `/etc/san/SANManager.template` is installed to preserve the existing `/etc/san/SANManager.cfg`.

  In this case, update manually the `/etc/san/SANManager.cfg` using the `.template` file.

Go to SAN Manager configuration file: /etc/san/SANManager.cfg, on page 3-1.

Installation of SAN Manager on Windows NT Servers

Delivery

The Windows NT directory of the SAN Manager CD–ROM contains the following components:

- SSMSetup.exe: SAN Manager agent for windows NT platforms.
- Java*: java runtime environment setup.

Prerequisites

Hardware required:

- a processor Pentium II 266 Mhz with at least 128 Mbytes of internal memory,
- a LAN connection,
- one or several Emulex LP 8000 FC adapters with firmware at level 3.02 min.

Software required:

The following software must be installed prior to install the SAN Manager Windows NT agent:

- Windows NT 4.0 with service pack 5 or later,
- Windows NT TCP/IP services,
- Java Runtime Environment version 1.2.2,
- Emulex SCSI Port driver.

The Windows NT server must communicate by TCP/IP protocol with the AIX server that plays the “Central Agent” role in the SAN Manager application.

Both the TCP/IP domain name system (DNS) and the naming via <lmhosts> and <hosts> files in the <%SystemRoot%\system32\drivers\etc> directory are supported as communication protocols.

Warning: The Emulex Configuration Tool must not be used for configuring LUNs Access Control on the Windows NT platforms with SAN Manager agent.

Installing Software on Windows NT servers

The software must be installaed in the following order:

1. Install the following prerequisite software:
   - Windows NT Service Pack (version = or > 5)
   - Windows NT TCP/IP Services
   - Java Runtime environment , see on page 2-5
   - Emulex_NT , see on page 2-4. note that the adapters must be installed before installing the driver.
2. Install the SAN Manager Windows NT agent:
   - global installation without ATF , see on page 2-6, or
   - global installation with ATF , see on page 2-7
3. Install ATF

Installing Emulex software

The Emulex software (Emulex driver for EMC products and its related “Emulex configuration tools”) must be installed prior to the SAN Manager Windows NT agent.

The Emulex software is delivered:

- by Bull within the “Fibre Connection Kits for DAS” for NT platforms connected to a DAS,
- on Emulex Web Site (http://www.emulex.com) for NT platforms connected to Symmetrix. Use the version “EMC Products”).

Note: If any version of the Emulex Software is – or has been – installed (Emulex basic, Emulex for EMC products or CLARiiON version) AND the LUN Access Control has been previously activated and/or deactivated through the ‘Emulex configuration tool’, OR if you don’t know weither or not these operations were done, you must clean the Emulex Software environment and install it again (see below).

To install the Emulex software, perform the following procedure:

1. Install the Emulex software.
2. Restart the Windows NT platform.
3. Select “Start Menu”.
4. Select “Program”.
5. Select “Emulex Configuration Tool”. The following window appears:

The figure above shows the main screen of the Emulex ‘configuration tool’: activate and/ or deactivate the LUN Access Control is done by checking the “Lun Mapping” box in the “Adapter Controls” area.

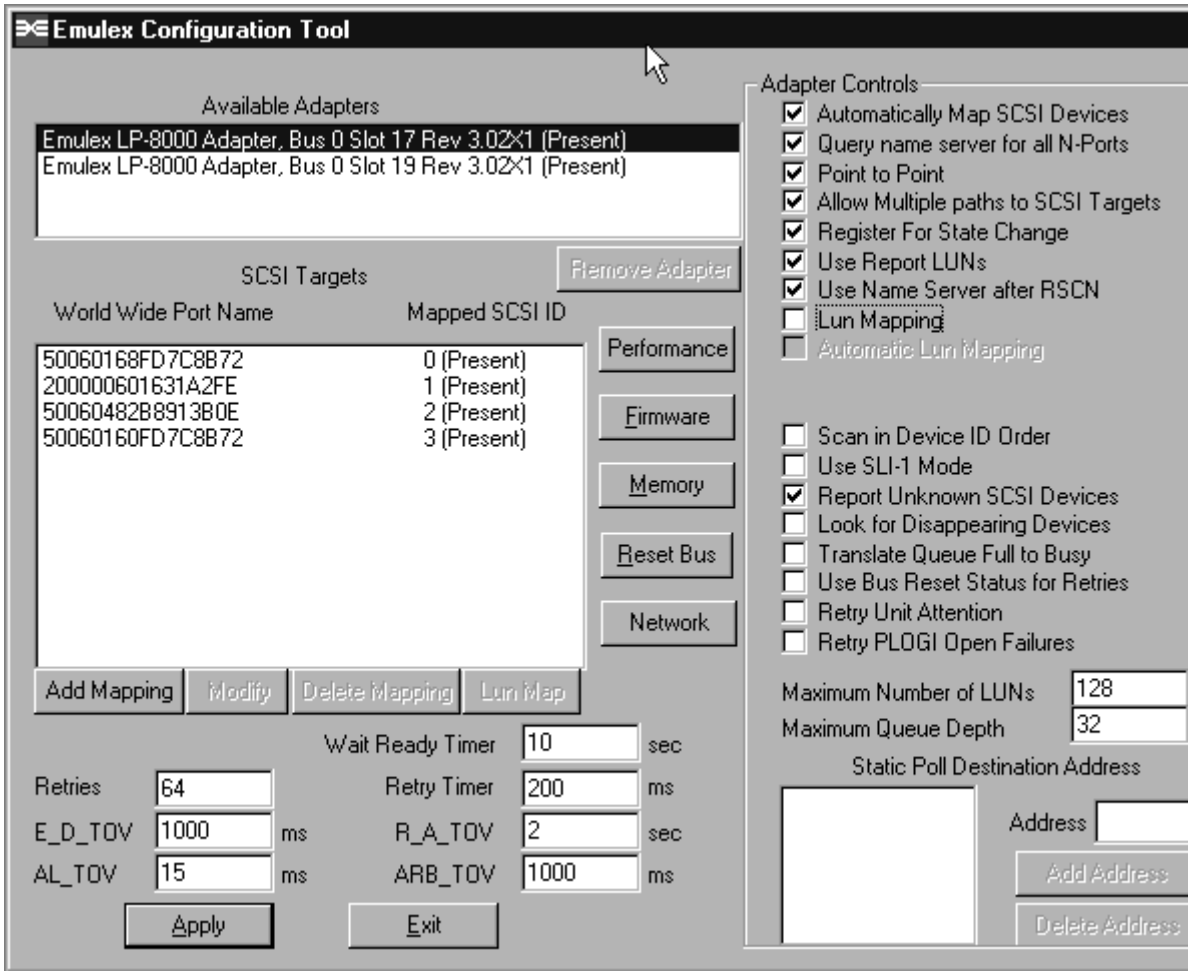


Figure 5. Emulex Software Tool window

6. For each adapter, check the settings corresponding to your SAN configuration.

Warning: Do not select the LUN mapping feature with this tool in any case. This would lead to unpredictable results when using the SAN Manager LUN Access Control feature.

7. Apply.

Installing the Java Runtine Environment

The Java Runtine Environment must be installed prior to the SAN Manager agent environment on all SAN Manager platforms. If it is already installed with the good level of version (refer to section ”SOFTWARE REQUIRED” , on page 2-3), skip this section else follow the procedure below:

1. Log on the Windows NT platform as a system administrator account.
2. Insert the SAN Manager CD–ROM
3. Start ‘Windows Explorer’ and select the <Windows_NT\`Java`> directory from the CD–ROM drive.
4. Double–click on the <*.`exe`> file and follow the instructions given in the different screens.

Global installation without ATF

Navisphere management application (NT Navisphere Manager or NT Navisphere Supervisor or AIX Navisphere Manager) uses an agent that can communicate with disk subsystems through the SAN with one or several LUNs.

But SAN Manager LUN Access Control can deny access to LUNs, in particular LUNs used by Navisphere agent: in this case, Navisphere management application cannot be operational.

To prevent that, it is recommended to dedicate some LUNs for Navisphere agent(s). These LUNs should contain no data and can be very small.

Access must be permanently allowed for LUNs dedicated to hosts that run Navisphere agent(s) and never be denied.

The following main installation steps should be followed for Windows NT platforms that will run a Navisphere agent:

5. Connect the hardware components.
6. If any, clean the Emulex driver environment and install the Emulex driver (refer to section ”Installing the Emulex Software ”, on page 2-4).
7. Install Navisphere agent (refer to the Navisphere documentation).
8. Create (using the Navisphere management application) as many LUNs as hosts where Navisphere agent runs: these LUNs will be dedicated to Navisphere activity.
9. Install the SAN Manager application (including NT SAN Manager Agents). See Installing the SAN Manager Windows NT Agent , on page 2-8.
10. Start the SAN Manager GUI (on one of the AIX servers) and allow access to each LUN to hosts where Navisphere agent are running (refer to Allow / Deny Access, on page 5-11. for detailed operations).
11. Reconfigure the Navisphere agent on each host where it runs:
    a. Start the ‘Navisphere Agent Configurator’.
    b. Clear device list.
    c. Auto Detect (the new device list). Detected host/SP link is displayed as follows in the ‘Navisphere Agent Configurator’ window:

```
Device                  Name            Description
\\.\SCSIv:x:y:z         SP_xxx  ...
```

    d. Save.
    e. Exit the ‘Navisphere Agent Configurator’.

Global installation with ATF

Note: LUNs must be mapped before ATF is installed. If a LUN mapping is performed after ATF installation, a reboot is needed for ATF to take in account the new configuration for versions equal or higher than ATF version 1.1.1. For previous ATF version, you must re–install ATF.

No special attention is required when using Navisphere, ATF and SAN Manager LUN Access Control, as in this case, the Navisphere agents do not require dedicated LUNs to run.

Keep in mind that SAN Manager is not aware of the presence of ATF. When a new disk subsystem LUN is allowed for access, SAN Manager only configures two paths if two hardware accesses are found at the time the mapping is started; at the end of the operation, one path is set “Available” (A) and the second path is set to “Defined” (D).

The following main installation steps should be followed on Windows NT platforms where ATF is to be used (these platforms must have at least two HBAs).

1. Connect the hardware components.
2. If any, clean the Emulex driver environment and install the Emulex driver. Refer to section ”Installing the Emulex Software ”, on page 2-4.
3. Install and configure Navisphere agent only.
4. Create (using the Navisphere management application) as many LUNs as hosts where Navisphere agent runs: these LUNs will be dedicated to Navisphere activity.
5. Install the SAN Manager application (including NT SAN Manager Agents). See Installing the SAN Manager Windows NT Agent , on page 2-8.
6. Start the SAN Manager GUI (on one of the AIX servers) and allow access to each LUN to hosts where Navisphere agent are running (refer to Allow / Deny Access, on page 5-11. for detailed operations).

   At this time, a double–mapping is automatically created by SAN Manager: the same LUN is now potentially accessible through the two HBAs.
7. Stop NT SAN Manager Agent (stopping the “S@N.IT!Scheduler” in NT services on platforms where ATF is to be installed (refer to ”Stopping SAN Manager processes” for detailed operations).
8. Install ATF on required hosts (refer to ATF documentation).
9. Re–configure Navisphere agent and ATF on each related host:
   a. Start the ‘Navisphere Agent Configurator’.
   b. Clear device list.
   c. Auto Detect (the new device list).

   At this time, detected host/SP links are displayed as follows in the ‘Navisphere Agent Configurator’ window:

```
Device          Name    Description
\\.\atf_sp0a            SP_xxx  ...
\\.\atf_sp0b            SP_xxx  ...
```

   d. Save.
   e. Exit the ‘Navisphere Agent Configurator’.

Installing the SAN Manager Windows NT Agent

Note: For the first installation of SAN Manager, clean the Emulex Software environment , on page 2-9, then re–install the emulex software, on page 2-4.

1. Log on the Windows NT server as a system administrator account.
2. Insert the SAN Manager CD–ROM.
3. Start Windows Explorer and select the “\Windows_NT” directory in the CD–ROM drive.
4. Double–click on the <SSMSetup.exe> file. The following window appears:

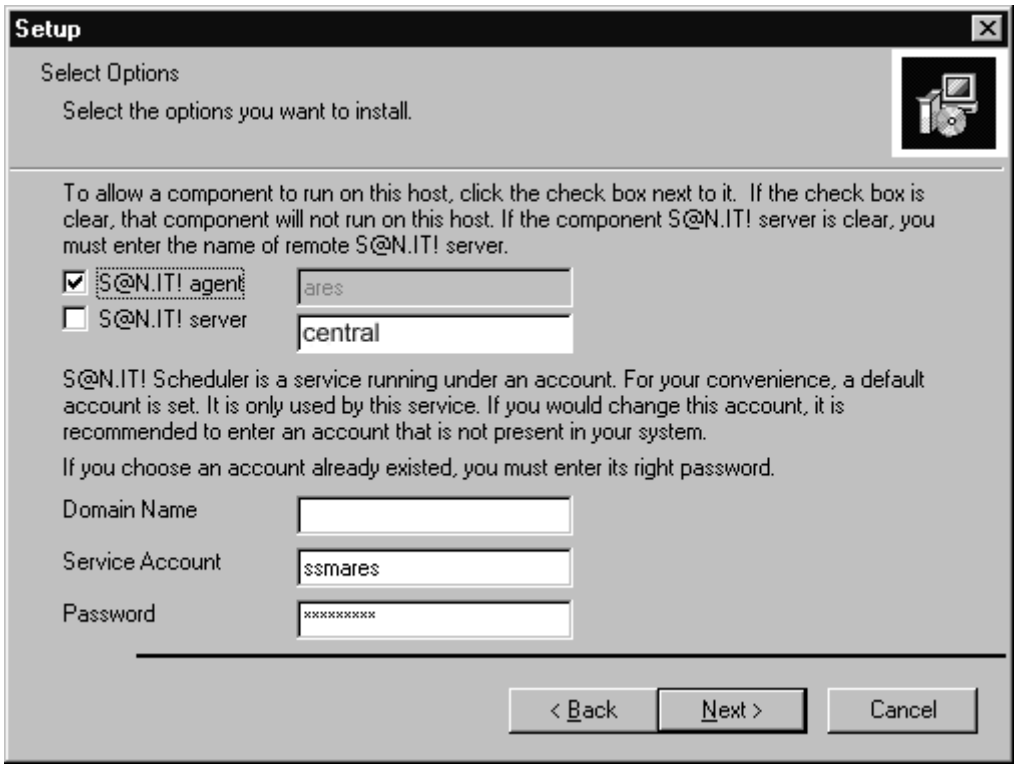


Figure 6. SAN Manager windows NT agent setup window

5. Follow the instructions given in the different screens and in particular:

   Check the S@N.IT agent box.

   Do not check the S@N.IT server box.

   Enter the IP name of the AIX platform with the central server role in the “S@N.IT!server” field.

   The following actions are done during the installation phase:

   – The SAN Manager.cfg configuration file (in the \Program–Files\Bull\S@N.IT\ directory) is updated
   – A NT user is created (to run the SAN Manager service). Default password = usename.
   – The ‘S@N.IT! Scheduler’ NT service is created and started. It launches the SAN Manager NT processes.
   – The LUN Access Control is activated on the current platform:
     – All LUNs of disk subsystems are made inaccessible. LUNs have to be explicitly mapped through the SAN Manager GUI.
     – All LUNs of non disk subsystems are made accessible; SAN Manager automatically map these LUNs.

Cleaning the Emulex Software environment

This operation MUST be done the first time the NT SAN Manager is installed (refer to section ”Installing the Emulex Software ”, on page 2-4 for details) or each time the LUN Access Control has been unfortunately activated and/or deactivated through the ‘Emulex configuration tool’.

The main operations to be done are:

1. If the Emulex Software is installed, remove it.
   a. Start>Settings>Control Panel>SCSI Adapters.
   b. Select the ‘Drivers’ tab.
   c. Select Emulex (or Clariion) driver.
   d. Click the ‘Remove’ button.
   e. Exit the Control Panel.
2. If the Emulex Software was installed, clean the Registry.
   a. Start>Run.
   b. Type “regedit” and click the ‘OK’ button.
   c. Enter the following directory key:

      My Computer
      HKEY_LOCAL_MACHINE
      SYSTEM
      CurrentControlSet
      Services

   d. Select ‘elxsli2’, right–click and ‘Delete’ the selection.
   e. Exit ‘regedit’.
3. Reboot the system.
4. Install the Emulex Software again, (refer to section ”Installing the Emulex Software ”, on page 2-4).
5. Reboot the system.

Un–installing the SAN Manager Windows NT Agent

1. Log on the platform as the same (as installation) system administrator account.
2. If you only upgrade NT SAN Manager agent go to step 3.

   If you plan to definitely remove it:

   – deny access to all LUNs now (refer to Deny Access, on page 5-13.

   – deactivate LUN Access Control (refer to Deactivate LUNs Access Control, on page 5-16.
3. Perform the standard Windows NT un–installation operation using:

   Start–>Settings–>Control Panel
   Add/Remove Programs...

Note: 'Ignore' all the following type of message that is displayed at the end of the un–installation processing:

```
|-------------------------------------------------------------
|Locked File Detected
|-------------------------------------------------------------
|An option you selected requires that files be installed to or
uninstalled from|your system, or both. A locked file,

 C:\Program Files\Bull\S@N.IT\,
|was found while performing the needed file operations.
|To leave this file as it is on your system, click the Ignore
button;
|to retry the file operation, click Retry; or to perform the
operation when your system is rebooted, click Reboot.
|
| | | Don't display this message again.|
|
|          | Reboot |   | Ignore |   | Retry |        | Cancel |
|-------------------------------------------------------------
```

4. Log off from the system administrator account.

The following actions are performed during the un–installation phase:

- **The LUN Access Control is not modified** on the current NT SAN Manager Agent platform. In addition:
  – The mapping of LUNs stays as is.
  – The 'S@N.IT! scheduler' NT service is stopped and removed and the NT user (for this service) is removed.
  – The shortcut is removed from the "Start" menu.
  – All files that have been installed are removed.

Note: The files dynamically created by NT SAN Manager are not removed.

  – The installation directory is not removed.

Chapter 3. SAN Manager Configuration File

Configuration File: SANManager.cfg

This file is located in the /etc/san directory on AIX servers, and in the installation directory (default=<%SystemDrive%:\Program Files\Bull\S@n.it\> on Windows NT servers.

This file specifies the configuration of the SAN Manager application. It contains two categories of parameters:

- Parameters that MUST be modified by the system administrator when the application is installed on a machine the first time:
  - Role of the current machine in the SAN Manager application.
  - IP addresses configuration (see also SAN Manager configuration and TCP/IP configuration, on page A-1).
- Parameters that can be left unchanged in most cases.

Each time the *SANManager.cfg* is modified, the SAN Manager application must be restarted for the modifications to be taken into account.

- using the */etc/rc.sanmgt start* command on AIX
- stopping and starting the “S@N.IT! Scheduler” NT service on NT platforms.

The syntax of the file must not be modified : lines that begin with a “ # ” are comments, others are of the form:

```
parameter_name=parameter_value
```

Note: There must be no space around the equal sign (“ = ”); uppercase and lowercase are not equivalent (including in “ yes ” and “ no ” values).

At the end of this chapter you will find an example of an AIX configuration data file, on page 3-4.

Basic Configuration

Role of the current machine

At least one of the `CentralRole, LocalRole, ClientRole` fields must be set to `yes`.

- `CentralRole`

  Must be set to `yes` on the AIX machine which is the central server.

- `LocalRole`

  Must be set to `yes` on machines connected to the SAN (i.e. the one that have Fibre Channel adapters) and on machines where the distributed AIX Navisphere Manager is launched.

- `ClientRole`

  Must be set to `yes` on AIX machines where the WebSM GUI server will be launched.

Warning: On Windows NT platforms, the only allowed role is “Local Role”.

IP adressing

- `MyHostname`
- `CentralHost`

Enter the name or the IP address, of the local server in the field `MyHostname=`, and the name or IP address of the central server in the field `CentralHost=`.

Note: The name or IP address is the same in both fields if the local server has also the role of the central server.

For more information, refer to SAN Manager configuration and TCP/IP configuration, on page A-1.

Advanced Configuration

Communication Configuration

- `CentralPort`

  Well known TCP port of the SAN Manager application on the Central Server. The value for this field must be the same on all the machines involved in the SAN Manager application.

- `ClientPort`

  TCP port used for internal communication between the different processes involved on a machine with `ClientRole=yes`.

- `LocalPort`

  TCP port used for internal communication between the different processes involved on a machine with `LocalRole=yes`.

Object Model Configuration (if `CentralRole=yes`)

- `ObjectModelPath`

  Name of the directory used to store information on a machine with `CentralRole=yes`.

Monitoring Configuration

- `MonitoringPeriod`

  if `CentralRole=yes` or `LocalRole=yes`

  Period (in seconds) of polling for the monitoring tools.

- `UserNotificationCommand`

  if `CentralRole=yes`

  Script to be called at each state modification of a SAN component detected by the monitoring. See file `/usr/lib/san/samples/NotifyCommand.template` for an example.

Warning: this script should have a restricted root access rights.

Topology Configuration

- `TopologyWindowWidth`

  Width of the window used to display the graphical topology (if `ClientRole=yes`).

- `TopologyWindowHeight`

  Height of the window used to display the graphical topology (if `ClientRole=yes`).

Log Configuration (if `CentralRole=yes`)

- `MonitoringLogFile`

  Name of the circular file where the state changes on the SAN components are logged (if `CentralRole=yes`).

- `MonitoringLogSize`

  Maximum size of the previous file in bytes.

- `AccessControlLogFile`

  Name of the circular file where the LUN access control changes are logged (if `CentralRole=yes`).

- `AccessControlLogSize`

  Maximum size of the previous file in bytes.

- `TraceDevice`

  There are two trace levels:

  – detailed (debug) messages

  – error messages

  This parameter may take three values:

  – 0 = only error messages are stored to the trace file.

  – 1 = all messages are displayed on the system console, and error messages are also stored in the trace file.

  – 2 = all messages (debug and error) are also stored in the trace file.

- `TraceDirectory`

  Directory that contains the circular trace files.

- `TraceSize`

  Maximum size of the trace files in bytes.

Launching the Application

Each time the *SANManager.cfg* is modified and saved on a machine, you must launch the application on this machine, using the following command:

`/etc/rc.sanmgt start` on AIX platforms.

stop and start 'S@N.IT! Scheduler' NT service on Windows NT platforms.

Starting SAN Manager Agents on the whole SAN

There is no requirements concerning the order in which the agents must be started.

It is possible to start SAN agents or client managers before or after the central agent.

It is however recommended to start the GUI only when all the agents have been launched.

/etc/san/SANManager.cfg Example on AIX Hosts

```
# AIX SAN Manager Configuration Parameters
# ========================================

# Application configuration
# -------------------------
CentralRole=no
LocalRole=yes
ClientRole=yes

# Communication configuration
# ---------------------------
# Hostname used for IP communication (it must be an active local IP
address)
MyHostname=csmgt12
# SAN Manager Central Server
CentralHost=csmgt13
# RMIregistry port of SAN Manager Central Server
CentralPort=38000
# socket port of SAN Manager Client
ClientPort=38001
# socket port of SAN Manager Local Server
LocalPort=38002

# Object Model configuration (if CentralRole)
# -------------------------
# Directory containing serialized files of the object model
ObjectModelPath=/etc/san/model/

# Monitoring configuration (if CentralRole or LocalRole)
# ------------------------
# Period of activation of monitoring (in seconds)
MonitoringPeriod=60
# User notification command (if CentralRole)
# This is a shell script to be called in case of status change
# detection of a SAN component.
# The following template can be used to write such a script:
# UserNotificationCommand=/usr/lib/san/samples/NotifyCommand.template
UserNotificationCommand=

# Topology configuration (if ClientRole)
# ----------------------
TopologyWindowWidth=600
TopologyWindowHeight=300

# Log configuration (if CentralRole)
# -----------------
# Monitoring log file name
MonitoringLogFile=/var/tmp/san/SANMonitor.log
# Monitoring log file maximum size (in bytes)
MonitoringLogSize=100000
# LUN Access Control log file name
AccessControlLogFile=/var/tmp/san/SANLunac.log
# LUN Access Control log file maximum size (in bytes)
AccessControlLogSize=100000

# Trace configuration
# -------------------
# trace redirection: 0=none 1=standard output 2=TraceFile
TraceDevice=0
# trace directory
TraceDirectory=/var/tmp/san
# trace file maximum size (in bytes)
TraceSize=50000
```

Chapter 4. Running SAN Manager Application

Running SAN Manager Application

This operation can be performed only on AIX machines with the `ClientRole=yes` in the */etc/san/SANManager.cfg* configuration file.

Starting a SAN Manager session

1. Start the WebSM framework by entering this command:

   ```
   wsm
   ```

   The WebSM ”launch pad” appears, as illustrated below.

Figure 7. WebSM entry window

2. Locate the “SAN Manager” icon and open it to start SAN Manager.

   The SAN Manager main window appears:

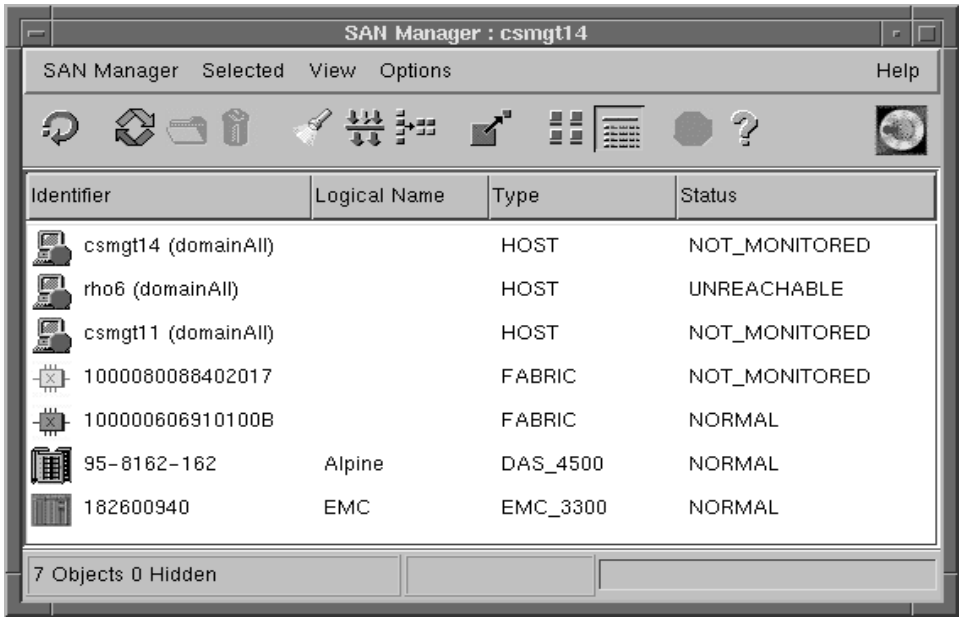


Figure 8. SAN Manager main window

In the SAN Manager main window, three types of SAN objects are displayed:

- the AIX and NT San agents of the current domain (domainAll initially),
- the fabric(s): this is the list of the fabrics visible in the current domain,
- the subsystem(s): this is the list of storage subsystems (Fibre DAS or Symmetrix) visible in the current domain (through switches, hubs or point–to–point connections).

Note: If this window remains empty, or if its content is incorrect or partial, check if the appropriate roles have been configured on each machine (see page 3-1), and if the corresponding agents have been launched by `/etc/rc.sanmgt`, (see page 3-3), on each AIX machine or “S@N.IT!Scheduler” on NT agent.

  – If the central agent is not running, the screen remains empty.

  – If the client manager is not running on the host where you run the GUI, the screen remains empty.

  – If the SAN agent is not running on some hosts, these hosts will not be displayed correctly, and some SAN components may be missing (or the host will be displayed as UNREACHABLE if it once had a SAN agent running).

SAN Manager Windows Overview

SAN Manager provides several different windows. You may switch from one window to another by:

- selecting a host or a subsystem and choosing the appropriate action in the 'selected menu',
- or moving the cursor in the Identifier field of a host or subsystem, and choosing the appropriate action by clicking on the right mouse button.

The possible transitions are described below:

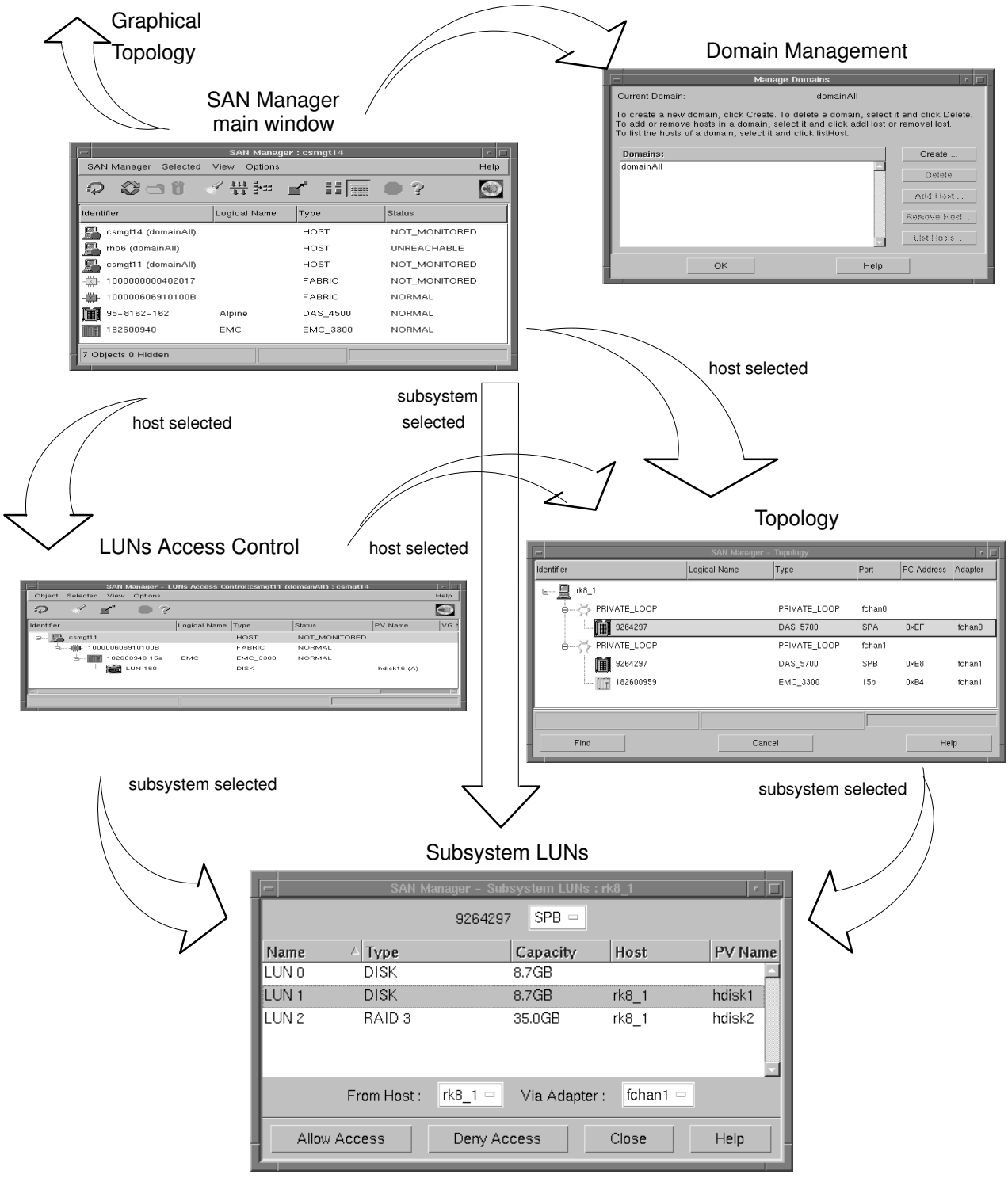


Figure 9. SAN Manager windows organization

Main Window Actions

The “SAN Manager” and the “Selected” menus from the menu bar provide actions which are respectively:

- global actions (concerning the whole SAN),
- object related actions (i.e. which apply to the selected object).

Note: Except for display actions, root authority is required.

The possible actions that may be performed from the main window:

- **From the “SAN Manager” menu (global actions):**
  - Display Graphical Topology, see page 5-2.
  - Select a Domain, see page 5-6
  - Manage Domains, see page 5-4
  - Run a snap on the Central Server, see page 5-22
  - Display the Event Log, see page 5-23
  - Display LUNs Access Control Changes, see page 5-10
  - Refresh Discovery, see page 5-24
- **From the ”Selected” menu with a host selected:**
  - Display LUNs Access Control, see page 5-7
  - Display Topology, see page 5-3.
  - Activate LUNs Access Control (valid if LUNs Access Control is deactivated), see page 5-15
  - Deactivate LUNs Access Control (valid if LUNs Access Control is activated), see page 5-16
  - Display LUNs Access Control Changes, see page 5-10
  - Run a snap, see page 5-22
  - Add this Host in Domain, see page 5-4
  - Remove this Host from Domain, see page 5-4
  - Delete a Host, see page 5-21
- **From the ”Selected” menu with a Fabric selected:**
  - Start Management Application, see page 5-17
  - Set Logical Name, see page 5-19
  - Display the Event Log, see page 5-23
  - Delete a Fabric, see page 5-21
- **From the ”Selected” menu with a Subsystem selected:**
  - Display Subsystem LUNs, see page 5-11
  - Start the Management Application, see page 5-17
  - Set Logical Name, see page 5-19
  - Display the Event Log, see page 5-23
  - Delete a Subsystem, see page 5-21

Help

A contextual help is available.

To open the help window, click on the ”Question Mark” icon.

Move the mouse over the different components to display the corresponding information.

This help is available on every window of the SAN Manager.

SAN Components Identification

The objects discovered on the SAN, and which are displayed in the main window are:

- hosts connected to the SAN via one or several Fibre Channel adapters
  - if the host is running SAN Manager agent, it is displayed with a “host” icon  and with an identifier which is the hostname of the machine.
  - if the host is not running SAN Manager agent,each adapter board is displayed with an “unknown host” icon  , and an identifier which is the World Wide Name associated to this board.
- fabrics, represented by a fabric icon  and identified by their World Wide Name.
- subsystems, which may be either:
  - Fibre DAS subsystems, displayed with a DAS icon  and identified as DAS_<model>
  - EMC2 Symmetrix subsystems, displayed with an EMC icon  and identified as EMC_<model>
  - other Fibre Channel disk subsystems (like DAE subsystems, or other suppliers FC disk subsystems): these objects are displayed as one “unknown disk” object per subsystem port, identified by the World Wide Name of the port and an “unknown disk” icon  .
  - SCSI tape or disk subsystems, connected via a CrossRoad SCSI–to–FC bridge: presently, only the first object discovered behind the CrossRoad bridge is displayed, identified by the World Wide Name of the bridge, and by an “unknown disk” icon  , or an “unknown tape” icon  .

  The SCSI to FC bridge itself is not displayed in the GUI.
- if several devices are connected together (not through a fabric), their connection will be shown as:
  - a single point–to–point connection if only two devices are found,
  - a private loop if more than two devices are found.

SAN Components Status

The status of a component may be:

- NOT_MONITORED: when it has been discovered on the SAN, but no monitoring is currently active. See Monitoring in Chapter 6-1.

  There is no monitoring for the AIX hosts. So, when an AIX host is reachable, its status is necessarily NOT_MONITORED.

- UNREACHABLE: when it is no longer reachable by SAN Manager:
  - in the case of a SAN host, the system may be down, or unreachable via IP, or the SAN agent may be stopped,
  - in the case of a fabric or subsystem, a cable may be disconnected; this may happen temporarily during network reconfiguration.

Once a fabric or subsystem is monitored (see Chapter 6.), its status will turn to:

- NORMAL: if it is monitored and no error is detected,
- FAULTY: an error has been detected by the monitoring daemon,

Refreshing the SAN Manager Display

Whenever a modification is detected, the currently opened windows are refreshed automatically (for all SAN Manager GUI instances currently running).

This happens when:

- modifications are made under SAN Manager. For instance, when the access of a LUN is modified, LUNs Access Control window is modified automatically,
- state modifications are reported by monitoring tools,
- modifications of SAN configuration have been detected,
- a `cfgmgr` is performed on an AIX SAN Agent.

However, even if SAN modifications are automatically detected by SAN Manager, it does not mean that AIX will work without any further administration. Refer to Modifying SAN Topology, on page 7-5 to know how to perform data–safe SAN modifications.

- An explicit refresh may be required by clicking the “Refresh Discovery” icon.

Note: Modifications that only impact a Windows NT platform may require 1 minute to be visible in the SAN Manager GUI.

Chapter 5. SAN Manager GUI

SAN Manager GUI Overview

This section describes the windows and the actions that may be performed within the SAN Manager GUI.

The windows available are:

- Main, on page 4-1.
- Graphical Topology, on page 4-1.
- Topology, on page 5-3.
- LUNs Access Control, on page 5-7.
- Set Logical Name, on page 5-19.
- Run a snap, on page 5-22.

The actions available are:

- Display Graphical Topology, on page 4-1.
- Display Topology, on page 5-3.
- Manage Domains, on page 5-4.
- Select a Domain, on page 5-6.
- Display LUNs Access Control, on page 5-7.
- Display LUNs Access Control changes, on page 5-10.
- Allow / Deny Access, on page 5-11.
- Activate LUNs Access Control, on page 5-15.
- Deactivate LUNs Access Control, on page 5-16.
- Start Management Application, on page 5-17.
- Set Logical Name, on page 5-19.
- Delete a Fabric, on page 5-21.
- Run a snap, on page 5-22.
- Display the Event Log, on page 5-23.
- Refresh Discovery, on page 5-24.

Display Graphical Topology

The graphical topology window displays all the SAN components. It is useful to have an overview of the complete domain.

Window Activation

To open the ”Graphical Topology” window:

From the SAN Manager main window,

select ”Display Graphical Topology” item of the ”SAN Manager” menu.

Two windows are displayed:

- A window representing all the SAN components of the currently selected domain appears.

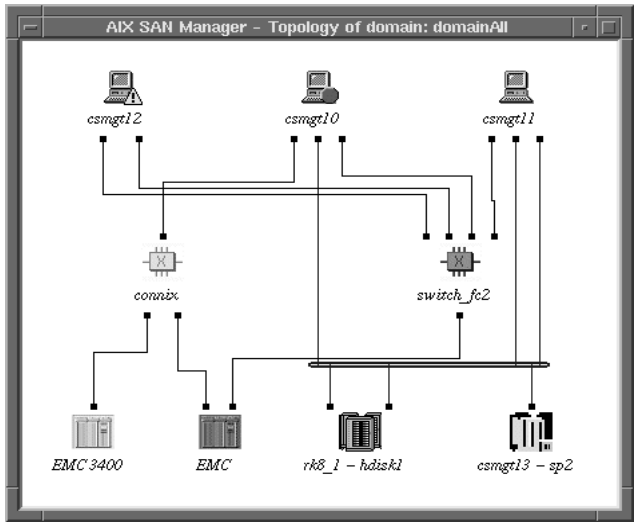


Figure 10. Graphical topology window

Moving the mouse over the different objects (hosts, fabrics and subsystems), a popup window appears displaying the properties of the selected object.

Note: The graphical representation is automatically refreshed each time the SAN Topology changes.

- A Control panel window is displayed allowing you to show all or parts of the SAN.

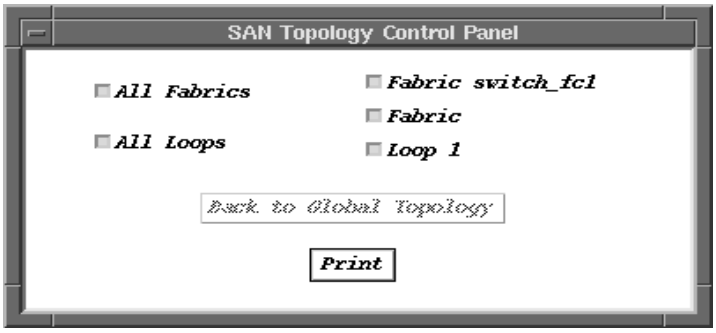


Figure 11. Graphical topology window

Note: This menu allows you to select loops and fabrics. If you want to select only specific hosts (i.e. display only a sub domain), you must shut the “Graphical Topology” window, select a domain in the “SAN Manager” menu of the main window, and re–launch the “Graphical Topology” window.

Display Topology

The topology window displays all the SAN components which are visible from a given host. It is useful to have an overview of the accessible subsystems, in order to define LUNs Access Control on a given host.

Window Activation

To open the ”Topology” window:

From the SAN Manager main window or from the ”LUNs Access Control” window:

Click on a host icon.

Select ”Display Topology” item of the ”Selected” menu.

A new window appears, containing all the SAN components which may be accessed from this host.

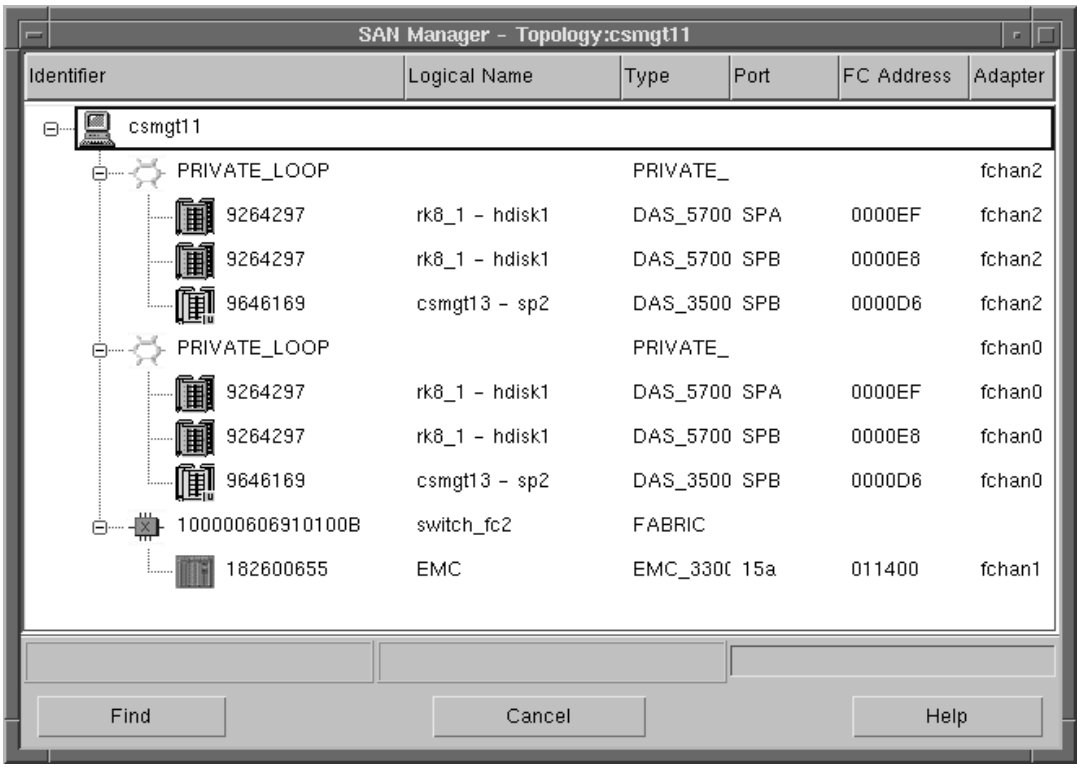


Figure 12. Topology window

Actions

Display Subsystem LUNs

This action opens the Subsystem LUNs window, which displays the list of the LUNs of the selected subsystem. In this window, the administrator may allow or deny LUN access.

For more information, see ”Allow / Deny Access”, on page 5-11.

Manage Domains

This action allows you to create or delete a domain.

When a domain is selected, you can add, remove a host, and list the hosts belonging to the selected domain.

Window Activation

To open the ”Manage Domains” window:

From the SAN Manager main window,

Select the ”Manage Domains” item of the ”SAN Manager” menu.

A new window appears:

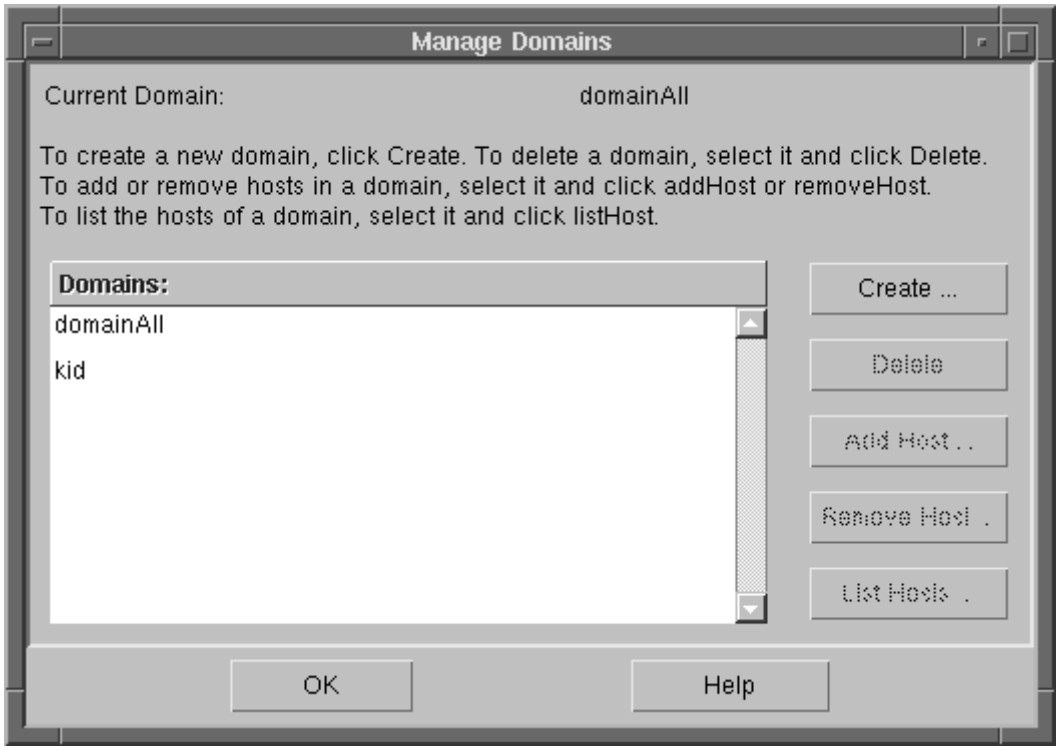


Figure 13. Manage Domains window

Create a Domain

This action allows you to add a domain. Proceed as follows:

- Click on the “Create” button. A new window is displayed.
- Enter a name of domain and confirm with the “OK” button.

A new domain is created.

Delete a Domain

This action allows to delete a domain. Proceed as follows:

- Select a domain in the list of existing domains.
- Click on the “Delete” button. A new window is displayed for confirmation.
- Click on the “Yes” button to confirm.

The selected domain is removed.

Add a Host

This action allows you to add a host to a domain. Proceed as follows:

- Select a domain and click on the “Add Host” button. A new window is displayed.
- Select the hosts to be added clicking on the list.
- Confirm by clicking on the “OK” button.

The selected hosts are added to the domain.

Note: You can also add several hosts together to a domain by selecting them in the main window and clicking on “Add this Host in Domain“ in the “Selected” menu.

Remove a Host

This action allows you to remove a host from a domain. Proceed as follows:

- Select a domain and click on the “Remove Host” button. A new window is displayed.
- Select the hosts to be removed clicking on the list.
- Confirm clicking on the “OK” button.

The selected hosts are removed from the domain.

Note: You can also remove several hosts together from a domain by selecting them in the main window and clicking on “Remove this Host from Domain“ in the “Selected” menu.

List Hosts

This action allows you to list in a new window the hosts belonging to a domain. Proceed as follows:

- Select a domain and click on the “List Hosts” button. A new window appears, displaying the hosts belonging to the selected domain.
- Click on the “OK” button to close the window.

Select a Domain

This action allows you to select a domain previously created with the Manage Domains action.

Window Activation

To open the ”Select a Domain” window:

From the SAN Manager main window,

Select the ”Select a Domain” item of the ”SAN Manager” menu.

A new window appears, displaying the list of all domains:

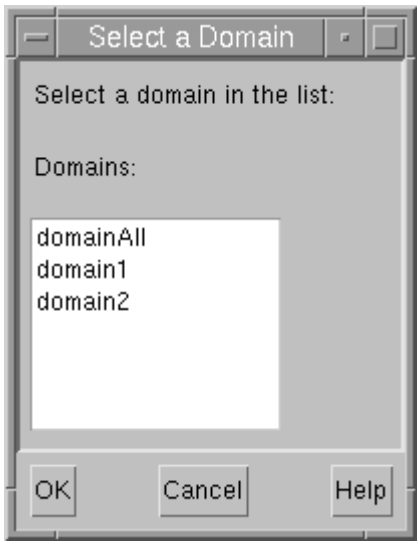


Figure 14. Select a Domain window

Select a domain and confirm by clicking the “OK” button.

Now the main window displays only the hosts belonging to the selected domain, and the SAN Components which are accessible from these hosts.

Any “Graphical Topology” window opened after this domain selection will show only the domain sub–view, but preexisting graphical topology windows will not be modified.

Display LUNs Access Control

This action allows the administrator to display the LUNs which are ”allowed”, see page 5-11, to be accessed by a given AIX SAN Agent host.

When the SAN Manager is installed, the LUNs Access Control is created empty and is ”inactive” on AIX SAN hosts, and “active” on NT hosts.

Until the Access Control mechanism is activated, see page 5-15, the AIX system continues to work as before and this screen is simply informative (displays the list of the LUNs already selected).

When the LUN Access Control is active, this screen displays exactly the part of the SAN which remains visible from the host selected.

Window Activation

To open the ”LUNs Access Control” window:

From the SAN Manager main window:

Click twice on a host icon.

or

Click on a host icon and select ”Display LUNs Access Control” item of the ”Selected” menu.

A new window containing the list appears.

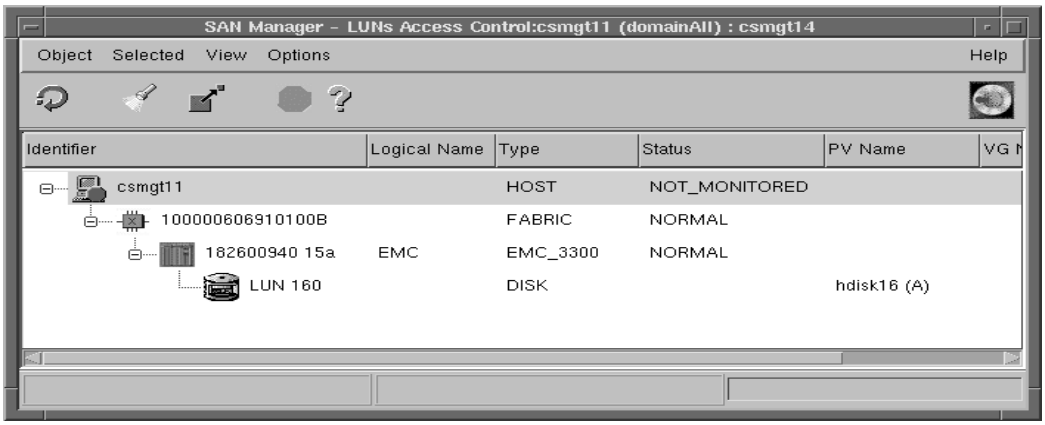


Figure 15. LUNs access control window

Depending on what you want to view, you may expand or contract objects by clicking on their associated “+” or “–” symbol. An object without a “+” or “–” symbol is a “leaf” of the tree, and cannot be expanded.

To add or remove physical volumes (LUNs) in the LUNs Access Control, see Allow /Deny Access, on page 5-11.

Fields Description

1. Identifier of the component.
2. Logical name: see Set Logical Name, on page 5-19.
3. Type: type of object managed (individual disk, RAID,...).
4. Status: UNREACHABLE, NOT MONITORED, NORMAL and FAULTY.
5. PV name:
   - on AIX: the name of the Physical Volume (PV) under which this LUN is known from AIX on the SAN Agent host,
   - on Windows NT: LUN number or disk number and its states (A=available, D=disable) when disk administrator has been launched.
6. VG name:
   - on AIX: the name of the Volume Group if any.
   - on Windows NT: the drive letter assigned to the disk (ex. C:).

Actions

Once the host is selected, you may:

Display Topology

The topology window displays all the SAN components visible from this host. It is useful to have an overview of the accessible part of the SAN in order to add LUNs to be managed by the SAN Manager.

To open the Topology window:

Click on the host icon.

Select ”Display Topology” item of the ”Selected” menu.

For more information, see ”Display Topology”, on page 5-3.

Activate LUNs Access Control

This action allows the administrator to activate the LUNs Access Control. It means that only the LUNs present in the LUNs Access Control will be visible and accessible to the host.

For more information, see ”Activate the LUNs access control”, on page 5-15.

Deactivate LUNs Access Control

This action allows the administrator to deactivate the LUNs access control. It means that all the LUNs present on the SAN are accessible to the host.

For more information, see ”Deactivate the LUNs access control”, on page 5-16.

Once a subsystem is selected, you may:

Display Subsystem LUNs

This action opens the Subsystem LUNs window, which displays the list of the LUNs of the selected subsystem and port and allows the administrator to allow or deny LUN access.

For more information, see ”Allow / Deny Access”, on page 5-11.

LUNs Access Control States

On AIX SAN Agent Platforms

The following figure shows that to change from inactive state to active state, a reboot command is needed on the AIX SAN Agent host after performing the “Activate” action.

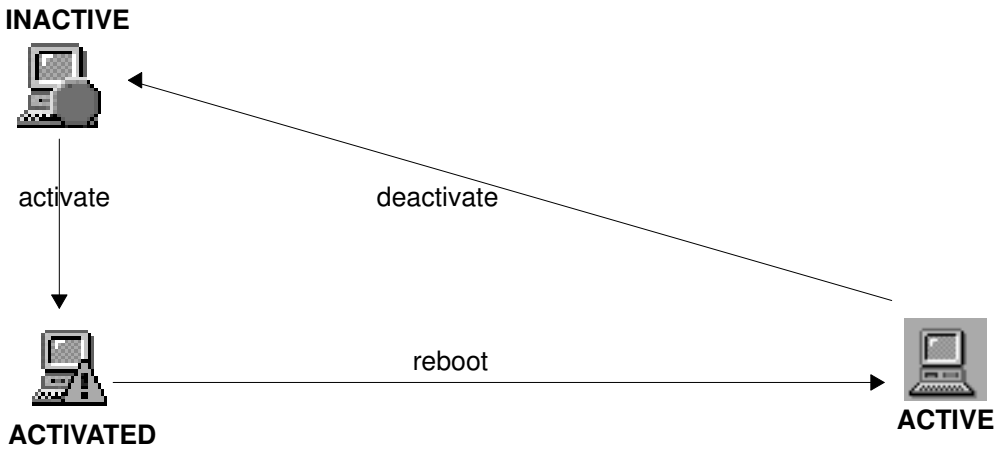
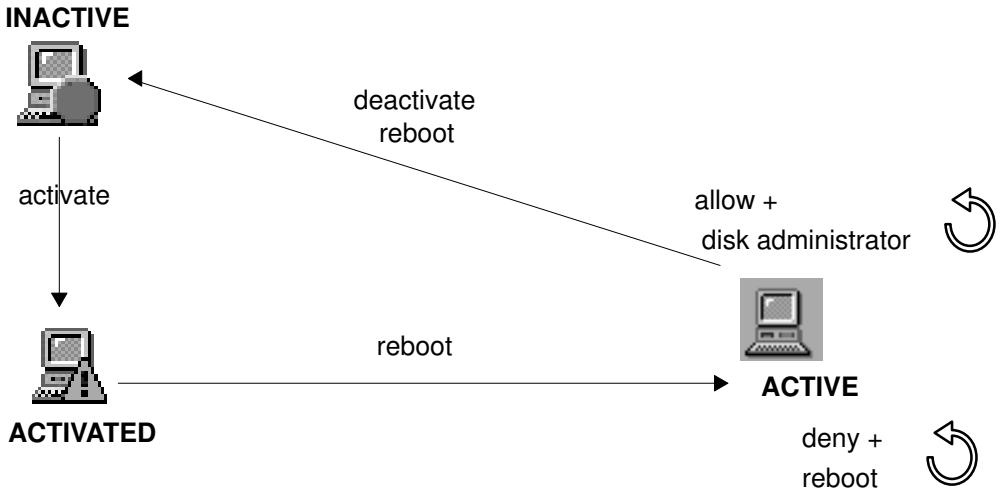


Figure 16. LUNs access control states.

On Windows NT SAN Agent Platforms

1. The initial state of the LUN Access Control after SAN Manager agent installation is ’ACTIVE’.
2. A reboot is mandatory after the following operation for the system to rebuild the disk tab:
   - after activation of the LUN Access Control (if it has been de–activated for some reason).
   - after de–activation of the LUN Access Control
   - after access to a LUN that has been denied to this platform
3. The NT Disk administrator must be launched after access to a LUN that has been allowed to this platform



Display LUNs Access Control Changes

This action allows the administrator to display the LUN Access changes. The changes are:

- Activate / deactivate LUNs Access Control.
- Allow / Deny Access to a given LUN on a given subsystem.

There are two possible views of this log:

- either at the central level, showing all changes performed on all SAN hosts,
- or at the local level, showing only the changes concerning a particular SAN host.

Window Activation

To open the ”LUNs Access Control Changes” window:

From the SAN Manager main window:

Select the ”Display LUNs Access Control Changes” item:

– either from the “SAN Manager” menu item to display the complete log,

– or from the “Selected” menu item after selecting a host, to display changes concerning this particular host.

A new window containing the LUNs Access Control changes appears.

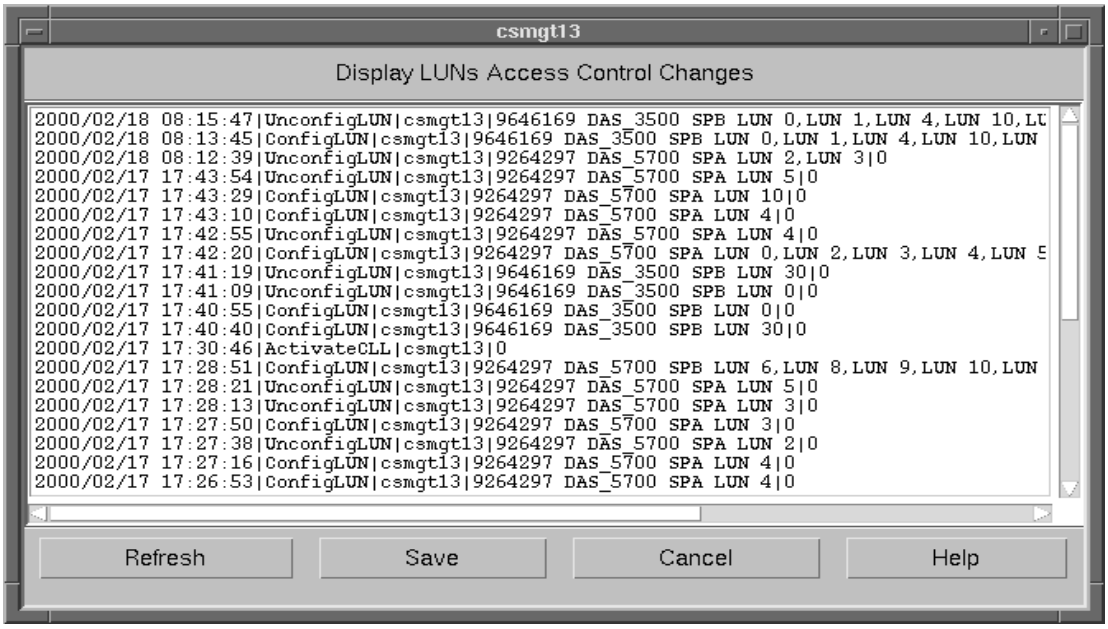


Figure 17. LUNs access control changes window

Use the refresh button to update this window.

Use the cancel button to close the window.

Allow / Deny Access

These actions allow the administrator to add or remove physical volumes (LUNs) into the LUNs Access Control list.

The LUNs Access Control is effective (i.e. only SAN components present in the LUNs Access Control are accessible to a host) when active.

If LUNs Access Control is inactive on a host, all SAN components remain visible and accessible until the next activation and reboot.

Opening the Subsystem LUNs Window

This window may be opened either from the main SAN Manager window or from the ”LUNs Access Control” window

Select a subsystem object.

Click on the subsystem and select ”Display Subsystem LUNs” item of the ”Selected” menu.

or

Select a subsystem and click on the right mouse button. Select ”Display Subsystem LUNsl” item.

The LUNs Subsystem window appears, containing the list of the LUNs of the selected Subsystem.

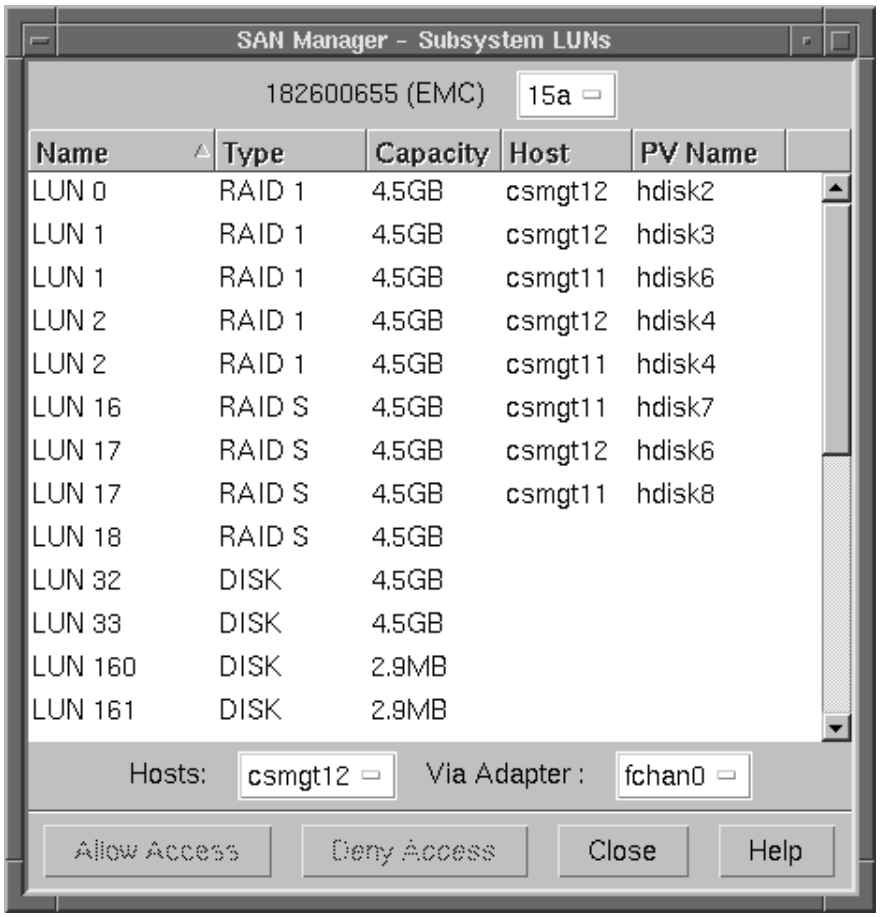


Figure 18. LUNs subsystem window

Description of the Window

1. Identification of the Subsystem whose LUNs are displayed below.
2. Port selector: allows to switch to the configuration of the LUNs of another port, if several ports are available to access this subsystem.
3. Fields:

   Name: the LUN identification in the subsystem .

   Type: type of object managed (individual disk, RAID,...).

   Capacity: size of the physical unit. Capacity = UNKNOWN means that the LUN is unreachable for the moment.

   Host: the name of the SAN Agent host which may access the LUN.

   PV name:

   – on AIX: the name of the Physical Volume (PV) under which this LUN is known from AIX on the SAN Agent host, and its state (A: available, D: defined, B: backup–ATF)

   – on Windows NT: LUN number or disk number ans its states (A=available, D=disable) when disk administrator has been launched.

   Note: Host and PV name are filled only for the LUNs already included in the LUNs Access Control of a host.

4. Host selector: SAN Agent host name. This selector displays all the hosts which are able to access this subsystem.
5. Adapter selector: allows you to select the adapter to be used to access the selected port of this subsystem when several paths are available. This selector is active only when no LUN of the subsystem is already configured (i.e. all the LUNs of a given part of the subsystem must be accessed by the same adapter).

Allow Access

To allow access to a LUN:

- Select a LUN (to add more that one LUN at the same time, maintain the Control key pushed and click on the LUNs.
- Check that the host selector displays the host to which you want to allow access.
- Click on the ”Allow access” button.

If the host is an AIX SAN agent platform

If the LUNs Access Control is active on the SAN Agent host (see ”Activate LUNs Access Control”, on page 5-15), the corresponding hdisk devices are automatically re–created under AIX.

When the “Allow Access” action is completed, the subsystem LUNs window is automatically updated, showing the Host name and PV name which have been associated with this LUN.

Note: Several hosts may be given access to the same LUN. In this case, there will be several lines for this LUN, each one concerning a different host (see for example LUN 17 in figure 18).

If the host is a Windows NT SAN agent platform

- A message like the following is displayed when a single path is detected:

```
Mapping of LUN 1 succeded on disk subsystem 1000020, type
DAS_5300, port SPB (A).

IMPORTANT:
        START THE DISK ADMINISTRATOR on host andromede NOW to
        terminate the operation.
```

- A message like the following is displayed when a double path is detected:

```
Mapping of LUN 1 succeded on disk subsystem 1000020, type
DAS_5300, port SPB (A).
Mapping of LUN 1 succeded on disk subsystem 1000020, type
DAS_5300, port SPA (D).

IMPORTANT:
        START THE DISK ADMINISTRATOR on host andromede NOW to
        terminate the operation.
```

- If the system Disk Administrator of the host to which access to the LUN has just been allowed, is running, stop it, and run it again to put a Disk signature.
- Create and format partition(s) within the new Disk# through the system Disk Administrator and assign them Drive Letter(s).

  Within one minute, the Disk # is displayed in the ‘PV Name’ field in the LUN Access Control window for the Host or Subsystem. In addition, if existing, the partition list is displayed in the ‘VG Name’ field.

Special configurations for multiple disk subsystem controllers.

If several controllers of the same disk subsystem are reachable, then the access to the LUNs is allowed for all the controllers the LUN is reachable through. The LUNs are “Available” on the controller they are assigned to and “Defined” on the other controllers. The same NT LUN number is assigned to each mapping of a particular FC LUN (but each controller is mapped to a different SCSI ID).

ATF Configuration (for DAS only).

LUNs must be allowed access before ATF is installed. If a LUN allow access is performed after ATF installation, a reboot is needed for ATF to take in account the new configuration for versions equal or higher than ATF version 1.1.1. For previous ATF version, you must re–install ATF.

Deny Access

To remove a LUN from the list:

- Select a LUN (to remove more that one LUN at the same time, hold the Control key down and click on the LUNs.
- Click on the ”Deny access” button.

If the host is an AIX SAN agent platform

If the LUNs Access Control is active, see ”Activate LUNs Access Control”, on page 5-15, the corresponding hdisk devices which were displayed in the PV Name field are removed from the AIX system, and hence no more available to users.

If the host is a Windows NT SAN agent platform

Before denying access, stop the disk access activity to the LUN, make sure the host does not currently use data, partition and logical disk of the related LUN and make sure the NT cache is flushed (you are advised to reboot the NT system to garantee the flushing and wait for the reboot completion).

Warning: because the NT cache is used to access data unpredictable results may occur if you deny access to LUNs where applications use the related data.

After Deny Access button has been clicked

- A message like the following is displayed when a single path is detected:

- ```
  Un-mapping of LUN 1 succeded on disk subsystem 1000020, type
  DAS_5300, port SPB.

  IMPORTANT:
      REBOOT the host andromede NOW to complete the operation.
      Do not start the Disk Administrator on host andromede before
  rebooting.
  ```

- A message like the following is displayed when a double path is detected:

- ```
  Un-mapping of LUN 1 succeded on disk subsystem 1000020, type
  DAS_5300, port SPB.
  Un-mapping of LUN 1 succeded on disk subsystem 1000020, type
  DAS_5300, port SPA.

  IMPORTANT:
      REBOOT the host andromede NOW to complete the operation.
      Do not start the Disk Administrator on host andromede before
  rebooting.
  ```

Warning: No reboot is needed to deny access to a LUN on NT itself. However a reboot is required for the operating system to rebuild its system disk map.

Special configurations for multiple disk subsystem controllers

If several controllers from the same disk subsystem are reachable, then the access to a LUN is denied for all the controllers the LUNs are reachable through.

Activate LUNs Access Control

This action allows the administrator to activate the LUNs access control on a SAN Agent host. It means that after the action is performed, only the LUNs present in the LUNs Access Control are accessible to the host.

To activate the LUNs Access Control, open the SAN Manager main window or the ”LUNs Access Control” window:

click on a host icon and select ”Activate LUNs Access Control” item of the ”Selected” menu.

or

select a host icon and click on the right mouse button. Select ”Activate LUNs Access Control” item.

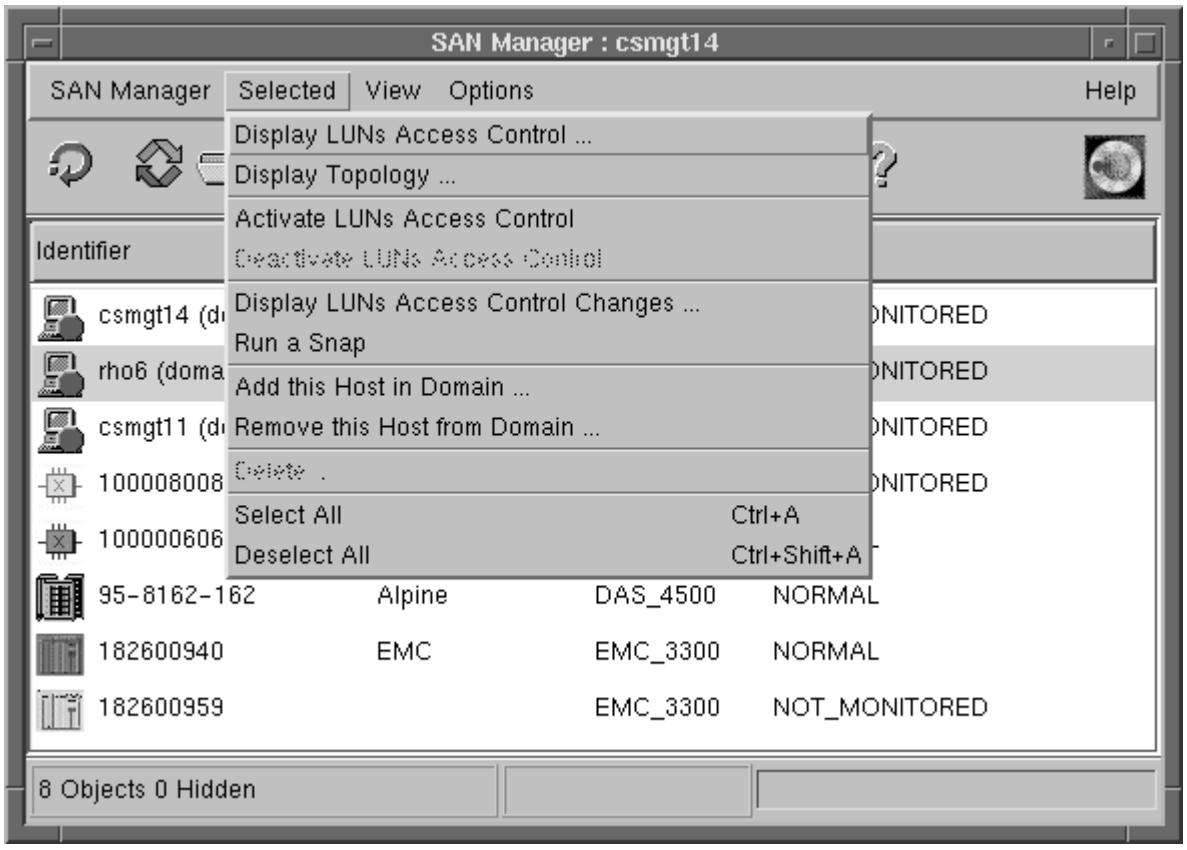


Figure 19. Activate LUNs Access Control

After performing the action, the LUNs Access Control is in an ’activated’ state. In this state, the host icon looks like  .

A reboot of the host must be done to make the LUNs Access Control ’active’. After this reboot, the host icon looks like  .

Warning: On NT platforms, a reboot is required for the operating system to rebuild its system disk map.

Deactivate LUNs Access Control

This action allows the administrator to deactivate the LUNs access control on a host. It means that all the LUNs present on the SAN subsystems are accessible.

To deactivate the LUNs Access Control, open the SAN Manager main window or the ”LUNs Access Control” window:

click on a host icon and select ”Deactivate LUNs Access Control” item of the ”Selected” menu.

or

select the host icon and click on the right mouse button. Select ”Deactivate LUNs Access Control” item.

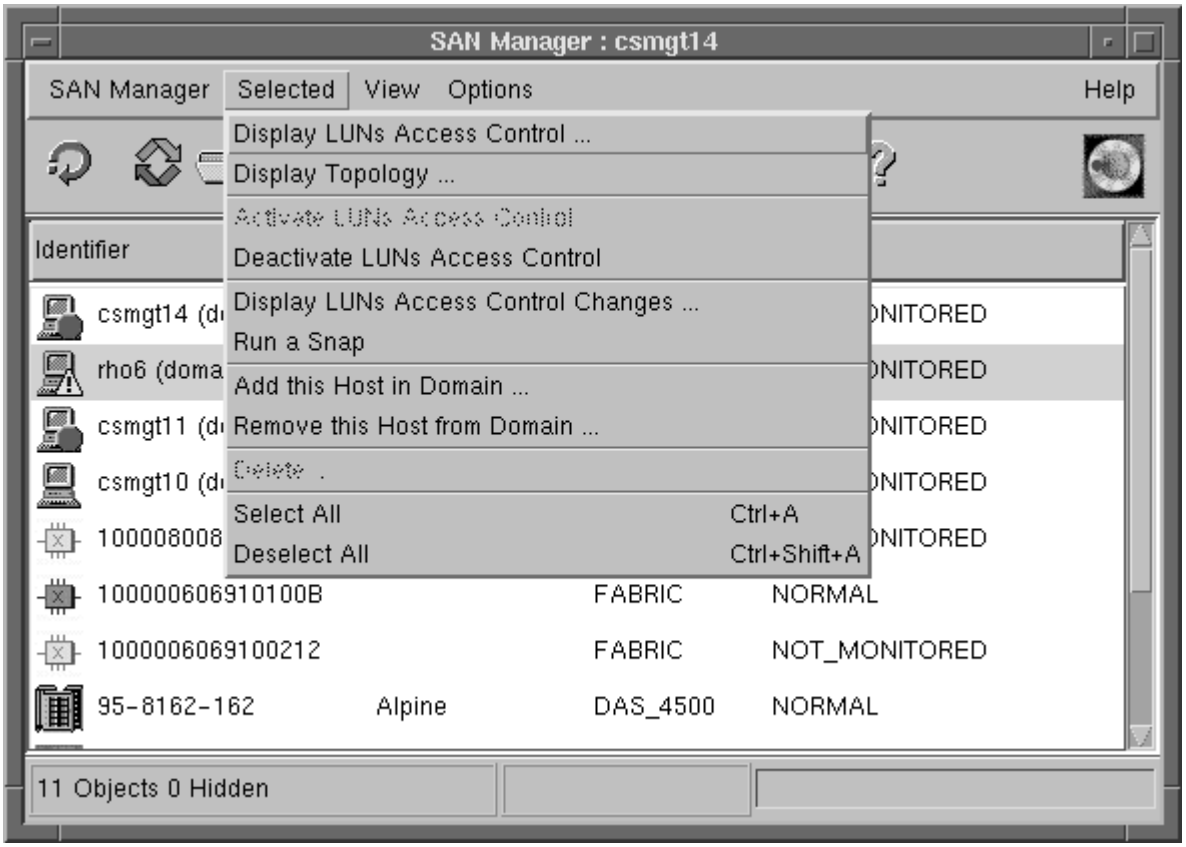


Figure 20. Deactivate LUNs Access Control

Note: after deactivation of the LUN Access Control, you must run a cfgmgr command (or reboot) to retrieve the hdisk devices to which access had been previously denied.

Warning: On NT platforms, a reboot is required for the operating system to rebuild its system disk map.

Start the Management Application

This action allows the administrator to run the management application of a SAN component.

Note: Root authority is required to run this action.

Select from the SAN Manager main window a fabric or a subsystem.

Warning: Launching of Management applications is possible only for applications that either run under AIX (AIX Navisphere Manager, Symmetrix Manager, telnet tool for switch) or those which have a web interface.

Running the AIX Navisphere Application for the Fibre DAS

To run the AIX Navisphere application for a DAS subsystem, proceed as follows:

- open the SAN Manager main window,
- select a Fibre DAS subsystem, 
- select ”Start Management Application” item of the ”Selected” menu,
- select the host where the Navisphere application is to be launched by selecting one from the list proposed.

Running the AIX Symmetrix Management Application for the SYMMETRIX

Prerequisites:

- Symmetrix Management application must be installed on the AIX SAN Agent,
- the selected subsystem must not be in the UNREACHABLE state.

To run the Symmetrix Management application:

- open the SAN Manager main window,
- select a Symmetrix subsystem, 
- select ”Start Management Application” item of the ”Selected” menu.

Note: 1. After the AIX Symmetrix Management application installation, in order to correctly execute Symmetrix Management commands from the SAN Manager, insert the following line in the `/etc/profile` file:

```
/usr/emc/ECC/symmappsrc.sh
```

where `/usr/emc/ECC/` is the installation directory for the Symmetrix Management application.

Note: 2. If you modify your Symmetrix subsystems after the Symmetrix Management application installation, you should run the following command:

```
$SYMMAPPS_DIR/bin/symmConsole -f
```

to force the Symmetrix Manager to perform a new discovery.

Running the telnet Tool for the Brocade Switch

To run the telnet tool for Brocade switch management application:

- open the SAN Manager main window,

- select a fabric, 
- select ”Start Management Application” item of the ”Selected” menu. If the fabric contains several interconnected switches, select the one you want to connect to,
- then ”telnet”.

A new standard telnet window appears.

Login as user admin.

Note: A switch does not allow more than one telnet connection at a time. Therefore you should not forget to close your telnet window when you have finished.

Running the Web TOOL for the Brocade Switch

Prerequisites:

- switchName must be set on the Brocade switch, and be the IP name associated to the switch.

  To set the switch name, proceed as follows:

  – launch the telnet session (see above),

  – login as ”admin”,

  – run the command `switchName ”<IP name>”.`

  `ex. switchName ”switch_fc1”` (quotation marks are mandatory).
- Netscape Navigator must be installed on the Client host.

To run the Brocade switch management application:

- open the SAN Manager main window,
- select a fabric, 
- select ”Start Management Application” item of the ”Selected” menu. If the fabric contains several interconnected switches, select the one you want to connect to,
- then ”Web tool”.

Set Logical Name

This action allows the administrator to set a logical name to identify fabrics and subsystems better.

Note: Root authority is required to run this action.

Running Set Logical Name Action

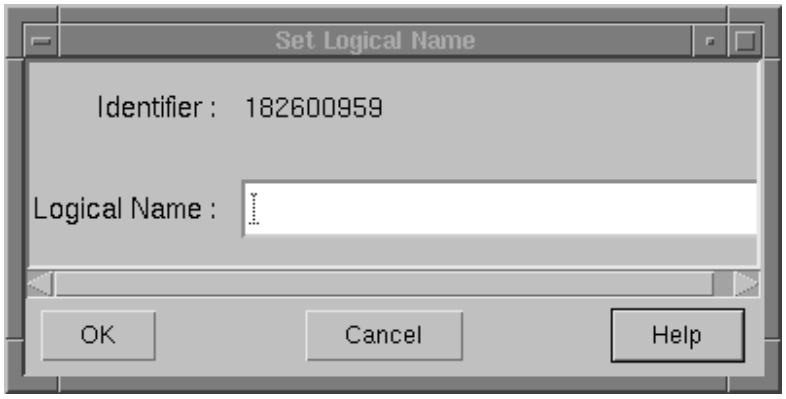
To activate the Set Logical Name, open the SAN Manager main window:

Click on a subsystem or a fabric icon and select ”Set Logical Name” item of the ”Selected” menu.

or

Select a subsystem icon and click on the right mouse button. Select ”Set Logical Name” item.

The following window is opened:



Logical Name Rules

If a logical name has been assigned to a subsystem via its own management application (Symmetrix Management or AIX Navisphere Manager), the SAN Manager will display this name directly.

But if this name contains special characters such as
”^”, ”|”, ”\”, ”/”, ”<”, ”>”, ”+”, ”*”, ”=”, ”&”, ”%”, ”:”, ”$”, ”?”, LF (line–feed) or CR (Carriage Return), those special characters will be replaced by ”_” (underscore).

Fabrics

A fabric consists of one or more switches. In case of Brocade switches, SAN Manager manages automatically the fabric.

A Logical Name is mandatory for monitoring (except for Brocade switch) or to launch the administrative application, and must be the IP name associated to the switch representing the fabric.

The Logical Name must be a valid IP name.

- If the switch is already accessible via IP, retrieve the Logical Name using the following command:

  ```
  host IPaddress
  ```

  Then, run Set Logical Name in SAN Manager.

- If the fabric is not accessible via IP:

– Retrieve the IP address, assigned at configuration time. It may be displayed on the control panel of the switch.

– Add an entry in the */etc/hosts*:

```
IPaddress Logical_Name
```

– Run Set Logical Name in SAN Manager.

Fibre Channel DAS Subsystems

Note: Logical Name is not mandatory.

- If AIX Navisphere manager is installed and has assigned a Logical Name to this subsystem, the logical name is automatically retrieved by the SAN Manager (see “Logical Name Rules” above).

  The Logical Name cannot be modified by the SAN Manager.

- If AIX Navisphere manager is installed and has not assigned a Logical Name:

  Run Navisphere application to assign a Logical Name (this name will be automatically retrieved by the SAN Manager).

  The Logical Name cannot be modified by the SAN Manager.

- If AIX Navisphere manager is not installed, a Logical Name may be assigned by the SAN Manager.

EMC Subsystems

Note: Logical Name is not mandatory.

- If AIX Symmetrix Management is installed and has already assigned a Logical Name: this name is automatically retrieved by the SAN Manager.

  The Logical Name cannot be modified by the SAN Manager.

- If AIX Symmetrix Management is installed and has not been assigned a Logical Name:

  Run Symmetrix Management application to assign a Logical Name in the ”Preferences” window of the Symmetrix Management (this name will be automatically retrieved by the SAN Manager).

  The Logical Name cannot be modified by the SAN Manager.

- If AIX Symmetrix Management is not installed on any SAN Agent, a Logical Name may be assigned by the SAN Manager.

Delete a Fabric, a Subsystem, or a Host

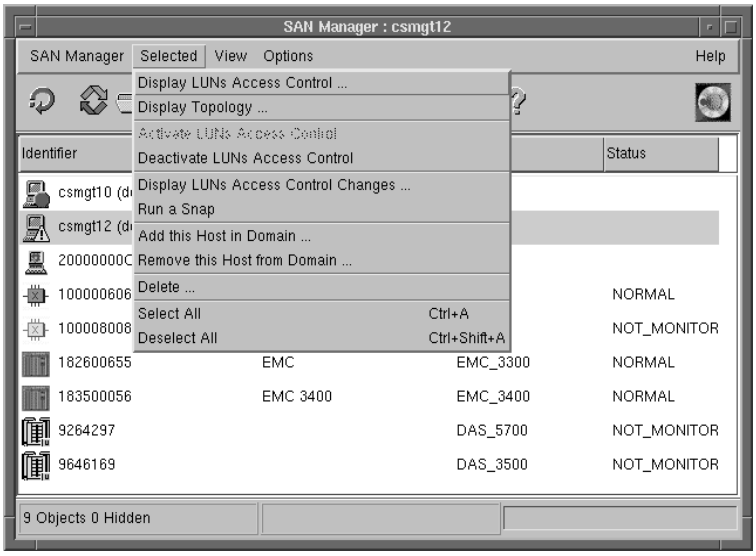


Figure 21. Delete a host

Delete a Fabric or a Subsystem

This action should be performed only when the administrator knows that the physical Topology has been changed and that the element (fabric or subsystem) has been removed from the SAN.

The corresponding component will disappear from the SAN Manager window.

If a deleted component is reachable again, it will reappear in the SAN Manager window.

To delete a fabric or a subsystem:

Select an UNREACHABLE fabric or subsystem in the Main window.

Select ”Delete” item of the ”Selected” menu.

Delete a Host

A host may be deleted only when no SAN Agent is running on it, or when it is disconnected from the SAN.

To delete a host:

Select an UNREACHABLE host in the Main window.

Select ”Delete” item of the ”Selected” menu.

Run a snap

Gathers information related to SAN configuration and creates a san_snap.tar.Z file in `/tmp/sanmgr.snap` directory on an AIX SAN Agent host or a Central Server.

To run a snap, from the SAN Manager main window, you can:

- click on the ”Run a snap on the Central Server” item of the ”SAN Manager” menu.

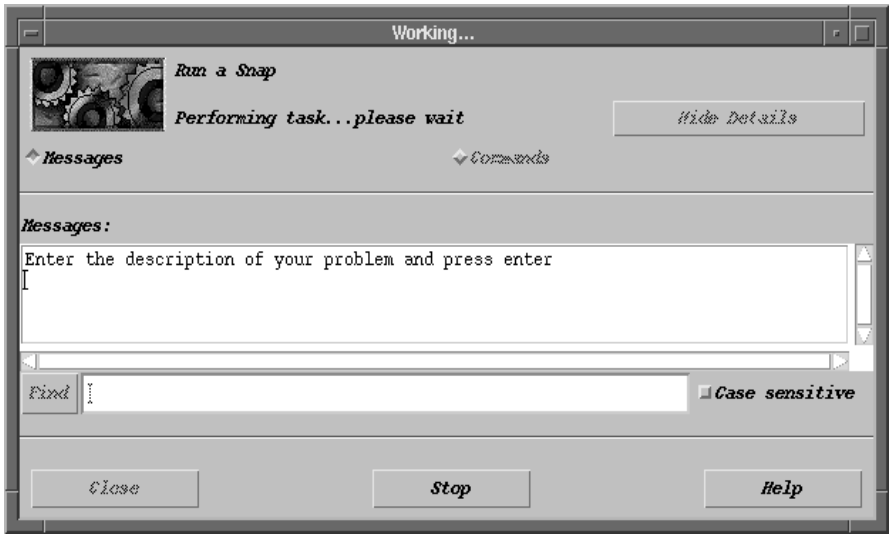
  The information will be retrieved and gathered on the Central host.

or

- select a AIX host, click on the ”run a snap” item of the ”Selected” menu.

  The information will be retrieved and gathered on the selected host.

A new window is displayed.



Enter the description of your problem and press Enter.

At the end of the process, click on the close button.

For more information about the snap command, see san_snap command, on page 8-1.

To gather information on a Windows NT platform, refer to the Reporting Procedure on a Windows NT SAN Agent, on page C-1.

Display Event Log

This action displays the status change events of the different SAN components such as fabrics (Brocade switches) and Subsystems (DAS, EMC).

Display Global Event Log

To display the global events:

From the SAN Manager main window:

- select a Host, Fabric or Subsystem,
- select ”Display the Event Log” item of the ”SAN Manager” menu.

A new window containing the events appears.

Figure 22. Event Log window

The output format is the following:

date, time, component type, component identifier, state, event description (including the name of the host that has detected the event).

Display Subsystem or Fabric Event Log

To display particular events:

From the SAN Manager main window:

- select a Fabric or Subsystem,
- select ”Display the Event Log” item of the ”Selected” menu.

Refresh Discovery

This action allows the administrator to update manually the main window.

Note: An automatical refresh discovery is done each time a modification of the SAN is detected.

To start the refresh discovery:

From the SAN Manager main window,

Select ”Refresh Discovery” item of the ”SAN Manager” menu.

Chapter 6. Monitoring

Monitoring Overview

Many Fibre Channel devices have their own manufacturer–provided management software. Some run on an AIX host connected to the SAN (like Navisphere for Clariion DAS, or Symmetrix Management or ECC for EMC2 Symmetrix). Brocade switch is a slightly different case, as the management software runs on the switch itself. Nonetheless AIX hosts may communicate with it, in various ways (telnet application, Brocade Web tool, SNMP requests, etc.).

There is a first level of integration, which is that all this software may be launched from the SAN Manager GUI. A system administrator who wants to display or modify some configuration details may simply select the appropriate device in SAN Manager main screen, then launch the management application.

This management software has another interesting feature, in that it checks the correct behaviour of the different devices. SAN Manager can communicate with the software to gather this information and display the status of the different components in the GUI. This is called monitoring.

Monitoring is not automatic: it requires a minimum of configuration which is described below. However it has a major interest in that it allows you to have a global, synthetic view of the whole network, and to check the availability as well as correct operating status of the devices; a malfunction is easily detected when the icon turns to orange–red. By clicking on this icon, you can then very easily launch the appropriate administration tool to detect the exact problem and correct it.

Monitoring also allows the SAN Manager to collect other interesting information:

- in the case of a Brocade switch, it can retrieve the World Wide Name of the switch, to check that it monitors the right object,
- in the case of the subsystem, it can retrieve the name already set in AIX Navisphere Manager, AIX ECC or Symmetrix Management, to use it as Logical name (insuring in this way coherency across various software tools).

DAS and Symmetrix subsystems, as well as Brocade fabrics, are initially displayed in the NOT_MONITORED state. It is only after initial configuration, and after a refresh delay of about 1 minute, that they switch to the monitored state: their status then appears as FAULTY or NORMAL whether an error has been detected or not.

If the configuration settings are changed, the status of the corresponding device returns to NOT_MONITORED, in order to let you know that errors may no longer be reported. These configuration settings are described below:

There should be only one monitoring source for each susbystem otherwise the monitoring status displayed for this subsystem may become inconsistent:

- for EMC2 symmetrix subsystems, there must be only one host where the “script on error” is enabled for this subsystem as described herafter.
- for DAS subsystems, the use of distributed AIX Navisphere Manager should be preferred to the use of multiple instances of AIX Navisphere Manager.

Fabric monitoring

Brocade fabric monitoring

The monitoring is entirely automatic and does not need any configuration.

Connectrix fabric monitoring

Give a logical name to the fabric: this name should be the IP name associated with the Ethernet address of the Connectrix switch representing this fabric.

Note: If the device at this IP address is not a Connectrix switch, it will not answer in the proper way and the state will become UNKNOWN.

EMC2 Symmetrix monitoring

Install the Symmetrix Management package on the AIX SAN Agent host chosen to manage the subsystem.

Define gatekeeper disks and start a poller for the subsystem (refer to Symmetrix Management documentation).

Launch SM–GUI, and then Window/Preference. In this window, modify the following fields:

- check the ”enable script on error” option,
- in the script name field, enter:

  `$SYMMAPPS_DIR/<identifier>/data/sannotifyerror`

  where `$SYMMAPS_DIR` is the Symmetrix Management directory.

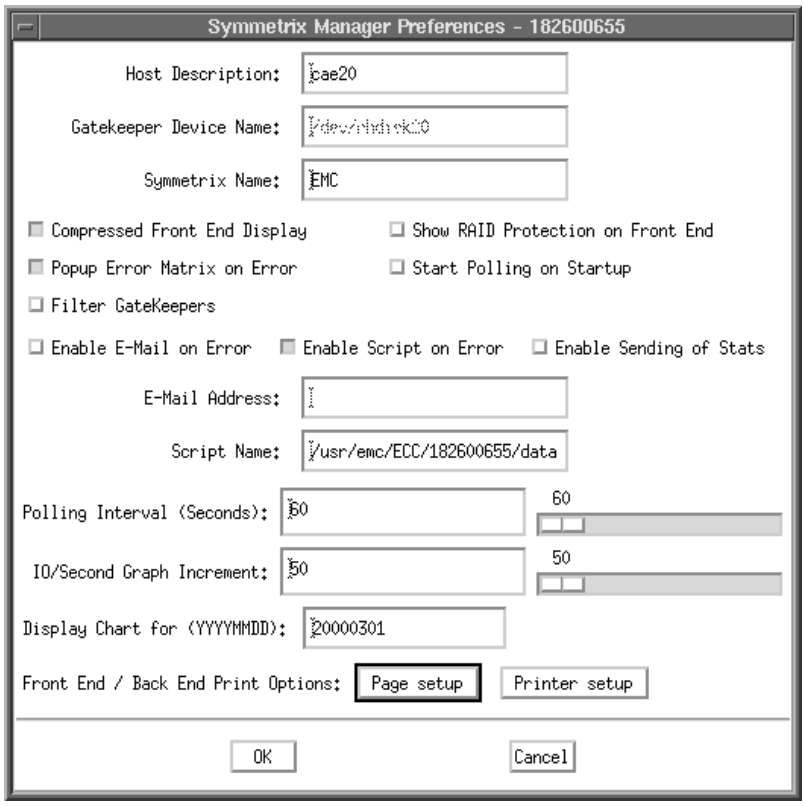
  example:

  ```
  SYMMAPPS_DIR=/usr/emc/ECC
  subsystem identifier = 182600655
  ```

  the script will be: `/usr/emc/ECC/182600655/data/sannotifyerror`

  you do not need to design such a script, it is provided by the SAN Manager.

  you may also choose a Symmetrix name (which will be used as Logical name by SAN Manager too).



Note: Symmetrix monitoring is only effective when the poller is launched. If you do not want to restart it manually every time your system is rebooted, add the appropriate commands in the `/etc/inittab` file.

Chapter 7. SAN Administration Guidelines

The SAN Manager tool has been designed to ease SAN administration, not to hide or suppress it. Administering such complex networks, requires specific attention.

This chapter highlights some of the important aspects of SAN administration as well as answers some of the questions that may arise in daily operations.

The following topics describe the administration of SAN Manager on AIX:

The following topics describe the administration of SAN Manager on Windows NT:

Using LUNs Access Control

SAN networks allow several hosts to view, and potentially access, the same data storage. Although possible (with adequate software), it is not the normal operating mode under AIX theoretically.

Thus, it is important, to decide which resources will be dedicated to which host, to set up LUNs Access Control lists accordingly on each host and to activate LUNs Access Control on all hosts as soon as you start the SAN network.

Managing AIX Volume Groups on SAN

Any host may handle volume groups and file systems on SAN storage subsystems, but several precautions are mandatory in order to handle this type of LUNs safely:

1. Use LUNs Access Control on all hosts to restrict visibility on the devices where volume groups reside. You may include in the SAN already existing volume groups and/or create new volume groups, even after the LUNs Access Control has been activated.
2. Precautions should be taken before shutting down the AIX system: Fibre Channel adapter addresses (AL–PA) are assigned by software and hence volatile: they may be dynamically assigned on a network at reinitialization time.

   These addresses are used by disk subsystems to identify the host that owns data on a disk (disk reservation). Therefore a host must free its reservations at shutdown time so as to be able to gain access to disks at reboot time, if a network reconfiguration has occurred in the meanwhile.

   The best way to achieve this is to edit the `/etc/rc.shutdown` file (which is executed at shutdown time) to stop related applications, unmount file systems and varyoff all SAN–based Volume Groups.

   If however, after an unexpected shutdown (power failure or system failure), access to LUNs can not be regained (i.e. the old device is in ”Defined” state, a new device has been created and any I/O access to this new device gives a ”busy” error message), disk access can always be recovered by shutting down the disk subsystem itself, rebooting it and performing a `cfgmgr` on the host: the disk reservation is not saved on a power–off / power–on on a disk or disk subsystem.

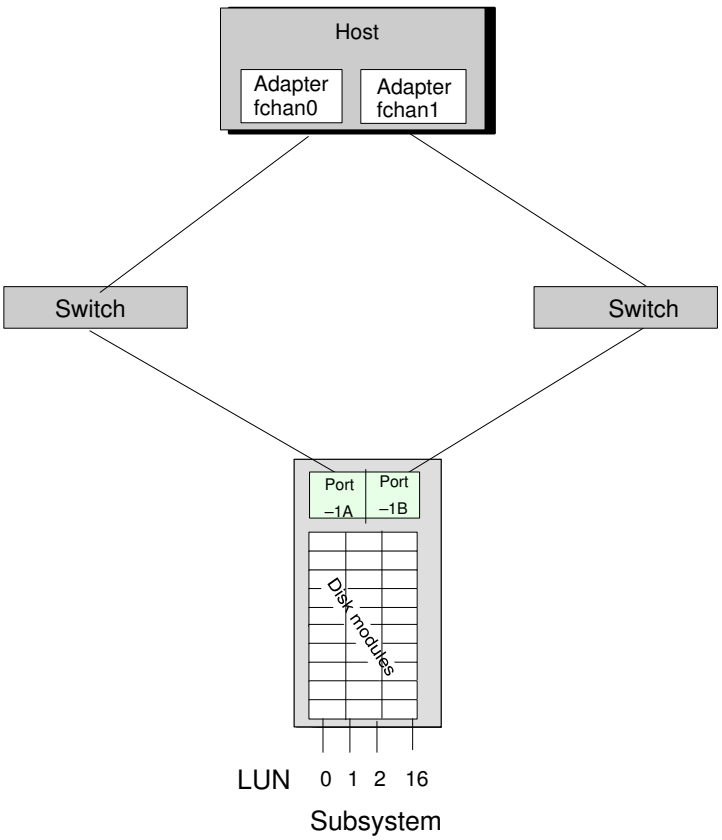
Managing Multiple Access Paths to a Subsystem on AIX

A SAN allows you to establish several access paths between any host and subsystem. This may be useful for:

- high availability (redundant connections),
- performance (optimization of the flow of data through the various connection paths)

This is quite an important evolution for AIX, which was originally designed to handle single connections of SCSI devices. Whereas a physical disk device was associated to a single hdisk device in AIX, a physical disk on a SAN may be associated, on a given host, to as many hdisk devices as there are paths between the host and the subsystem.

For example, if a host has the connections illustrated below:



An `lsdev -C` on this host will show the following:

```
fchan0  Available    04-01           PCI Fibre Channel Adapter
fchan1  Available    04-02           PCI Fibre Channel Adapter
fcp0    Available    04-01-3M        Fibre Channel FCP Interface
fcp1    Available    04-02-3M        Fibre Channel FCP Interface
hdisk2  Available    04-02-3M-0,0    SYMMETRIX RAID-1(local)
hdisk18 Available    04-01-3M-0,0    SYMMETRIX RAID-1(local)
hdisk3  Available    04-02-3M-0,1    SYMMETRIX RAID-1(local)
hdisk19 Available    04-01-3M-0,1    SYMMETRIX RAID-1(local)
hdisk4  Available    04-02-3M-0,2    SYMMETRIX RAID-1(local)
hdisk20 Available    04-01-3M-0,2    SYMMETRIX RAID-1(local)
hdisk6  Available    04-02-3M-1,0    SYMMETRIX RAID-S(local)
hdisk21 Available    04-01-3M-1,0    SYMMETRIX RAID-S(local)
.
.
```

`fchan0` and `fchan1`: the two adapter boards

`fcp0` and `fcp1`: the two FC ports of the disk subsystem

`hdisk2` and `hdisk18`: LUN 0; `hdisk3` and `hdisk19`: LUN 1; `hdisk4` and `hdisk20`: LUN 2; `hdisk6` and `hdisk21`: LUN 16; ...

Note that the x,y part of the location field in the `lsdev -C` output is a ”SCSI like” transcription by AIX of the LUN number:

x = LUN / 16 (quotient of the integer division of the LUN number by 16)

y = LUN % 16 (remainder of the previous integer division)

The example shown here may look simple but it is clear that if you have a lot of redundant access paths, and several disk subsystems connected to the SAN, a lsdev –C will become more complicated, especially because you will not get lines nicely sorted as above.

SAN Manager greatly eases this administration, in that it gives a LUN–consolidated view of the storage devices, and displays the correspondance between LUNs and hdisks. It also allows you to reduce the total number of hdisk devices to those which are really needed on each host.

But there are still some administration issues which are related to multiple accesses on SAN network, and which should be considered with care.

Whether you have multi–connected a DAS or a SYMMETRIX, the situation will be different as detailed below:

Managing Multiple Paths to a DAS Subsystem

There are two Fibre Channel ports on each DAS subsystem. In most of the cases, both connections are used.

But there is no real redundancy, as a DAS subsystem allows any individual disk device to be visible through one path only.

What is seen on the AIX side depends on whether ATF is installed or not on the given host.

Although you may set two physical paths to a given DAS subsystem, there will never be more than one active path at a given time for each LUN, only one hdisk is visible for each LUN. ATF keeps the same hdisk but switches automatically from one path to another if the first path fails.

Managing Multiple Paths to a SYMMETRIX Subsystem

There is a variable number of access points (called Channel Directories) to a SYMMETRIX disk subsystem: from 2 to 64, depending on the number of communication adapters that are used on the server.

Any LUN of the subsystem may be made ”visible” through several channel directories simultaneously.

On a host which has access to these channel directories, each LUN will be associated to several hdisks (one for each communication path), all in the ”Available” state.

- If PowerPath is installed, it will define hdiskpower devices on top of hdisks: there will be one hdiskpower device per LUN. You now define volume groups on hdiskpower devices, and let the PowerPath decide which path it uses to access LUNs.

  This is the most efficient way, as PowerPath will use alternatively all paths, with the load balancing policy of your choice. If you use LUNs Access Control, you should select LUNs on all the different paths to the EMC subsystem.

- If you do not use PowerPath, you must use LUNs Access Control to restrict access to each LUN to only one path.

Multiple Paths and Volume Groups

When a volume group is mounted, AIX associates it with one specific path (use `lspv` and `lsdev -Cc` to check that).

If this path fails without a multiple path manager (ATF or powerpath, you may have problems to recover your volume group through another path.

In this case, perform an `rmdev -dlR` on the fchan associated with the failed path, then a `cfgmgr` to solve the problem. Do not forget to update the fchan topology if you work in point–to–point mode.

Using Zoning with SAN Manager

Zoning allows you to create segmentation or zones, within a fabric, that comprise selected hosts and storage subsystems.

Zoning limits access of information to only the devices in the defined zone.

- Fabric zones are not displayed in SAN Manager.

- GUI display may or may not be modified, depending on the zoning topology.
  - if SAN Agent hosts can access the whole fabric (for instance, if there is a SAN host running a local agent in each zone), there is no modification with zoning: all devices are seen.
  - if SAN Agent hosts cannot access the whole fabric, some SAN components may be incompletely identified: they will be displayed in the GUI as “unknown hosts”  (whether they are hosts or subsystems).

If you want to suppress these useless objects, define a domain containing only the SAN hosts, and select this domain: “unknown hosts” will not be displayed any more.

Compatibility with Access Logics (DAS) or Volume Logix (EMC)

These software products provide another means of LUNs Access Control, on the subsystem side.

This may look redundant with SAN Manager, which performs LUNs Access Control on the host side.

However, it may be useful to have these products running together, for instance if you mix AIX and NT hosts with other kinds of hosts, or if you want to take advantage of SAN Manager’s other capabilities, like monitoring or graphical topology, along with Access Logics or Volume Logix LUNs Access Control.

These software products are not incompatible with SAN Manager, provided that they are correctly configured.

A mandatory requirement for SAN Manager is that all SAN hosts must see the same LUNs on each subsystem port (otherwise, the subsystem LUNs window would not be reliable).

Hence, Volume Logix and Access Logics should give the same access rights to all SAN hosts, and further LUN access limitations should be configured via SAN Manager.

Modifying SAN Topology

On your SAN, you may want to connect new subsystems or hosts, remove obsolete ones, or replace elements. You may also want to temporarily modify the connections (in case of a hardware failure for instance).

It is important to proceed in the way described below in order to keep a coherent SAN Manager display, as well as a correct AIX or NT behaviour.

Adding a Component (switch, hub or subsystem)

1. Connect the component.
2. Run `cfgmgr` on all AIX SAN Agent hosts that are connected to it. Reboot the NT servers that are connected to it.

The added components will appear in the Main and Topology SAN Manager windows.

3. Update the LUNs Access Control (Allow Access) on these hosts.

See also Adding a New Subsystem to the SAN, on page 7-10

Temporarily Disconnecting a Component (switch, hub or subsystem)

If you temporarily disconnect a component or if a component is temporarily out of order, there is nothing to do. On Windows NT platforms, the SAN Manager performs a refresh periodically.

- SAN Manager GUI is automatically refreshed.
- Components associated to the lost connection switch to UNREACHABLE state (orange icon).

Reconnecting a Component (switch, hub or subsystem)

If you reconnect an already existing component in its original slot (that is in the UNREACHABLE state), there is nothing to do. An appropriate signal will be sent on the SAN, FC AIX driver and then SAN Manager are notified of the event, and SAN Manager GUI is refreshed: the components associated to the reconnected device will switch back to their previous state:

- NOT_MONITORED
- NORMAL or FAULTY if the components are monitored

Note: Always run `cfgmgr` and not simply `cfgmgr -l fchan<x>`, otherwise the SAN discovery will not be launched at the end.

Removing a Component (switch, hub or subsystem)

When a component is disconnected, there is no way for the SAN Manager to know if this disconnection is permanent or not. That is why it simply appears with an orange–red icon and an ”UNREACHABLE” state.

If you want to remove a component (for instance unplug a subsystem to plug it somewhere else), the following tasks must be performed to recover your data without problems:

1. Identify all volume groups to which you will lose access.
2. Unmount any file systems, and varyoff volume groups.
3. Remove all related AIX devices with the `rmdev -dRl` command.

   ```
   rmdev -dRl fcp5
   ```

Note: You will have to stop Navisphere by running `/etc/rc.navi stop`, to be able to remove DAS devices.

4. Disconnect the cables. SAN Manager GUI is automatically refreshed: all related components switch to the UNREACHABLE state.
5. In the SAN Manager GUI main window, select the UNREACHABLE component, and delete them (see Delete a Subsystem, on page 5-21).

Note: The deleted components will disappear from the Main, LUNs Access Control and Topology SAN Manager windows.

Modifying Component Connections

If you want to unplug a component, and replug it somewhere else on your SAN, proceed as follows:

1. Remove the components whose connections will be modified, performing the steps described in the above section: ”**Removing a Component**”.
2. Add the components with the new connections, as explained before in the ”**Adding a Component**” section.

Adding a host to the SAN

All hosts connected to the SAN through SAN interconnect components (such as fabrics or private loops for example) have the visibility of Logical UNits (or LUNs) of all SAN peripheral devices and especially LUNs of SAN disk subsystems. Without specific mechanism, access is potentially possible from these hosts to those LUNs and may lead to data corruption.

So no host should be connected to the SAN before the following operations have been performed on this host:

- the **ASM SAN agent software has been installed,**
- the **LUN access control mechanism has been activated**.

For Windows NT hosts, a reboot is required after the installation of the ASM SAN agent.

For AIX hosts, the activation of the LUN access control mechanism thru the ASM GUI and a reboot of the host are required.

Procedure to add a Windows NT host to a SAN managed by ASM:

The target is to have a new Windows NT host operational through the SAN.

- We assume that the initial state is the following one:
  - a SAN exists,
  - one or several ASM SAN agent platform(s),
  - the ASM server and ASM GUI are running,
  - LUNs dedicated to the new host have been created,
  - **the new host is not connected to the SAN**.
- The installation of the ASM SAN agent for Windows NT is to be performed off–line (no hardware connected to the SAN) in order to mask existing LUNs to the new host.
- The main steps of the installation are the following. Refer to *AIX SAN Manager User's Guide* for details on each operation.

3. Install the operating system. Connect the host to the LAN and configure the TCP/IP services.
4. If needed, clean the Emulex driver environment.
5. Install the appropriate Emulex driver.
6. If needed, install Java runtime.
7. Install ASM SAN agent for Windows NT. Within one minute, the new host appears in the ASM GUI.
8. Connect the host HBA(s) to the SAN.
9. Map LUNs for the new host (and especially the LUN to be used by the Navisphere agent if any).
10. If a LUN is to be used by the Navisphere agent, stop ASM SAN agent on the new host and install Navisphere agent and ATF. Reconfigure Navisphere agent and ATF. Finally, re–start ASM SAN agent.

Removing a host

If a host is stopped, or no more accessible, it can be removed from the SAN Manager.

MSCS Cluster LUN access control

Access to the LUNs corresponding to Cluster Shared Disks must be allowed to both nodes of MSCS Cluster, **and can be allowed to these Cluster nodes only**.

Protection against concurrent access is achieved by MSCS.

Prerequisite to MSCS installation, there must be at least one LUN shared by Cluster nodes, for having at least one NT Disk to share.

Once MSCS is running, LUNs may be added to the Cluster without interrupting applications under MSCS control, using the following steps:

1. Create and bind relevant LUN(s) using Navisphere.
2. Allow access to the LUN(s) to one host (ex: Node1) using SAN Manager graphical interface.
3. It is recommended to reboot Node1 when ATF is used. Applications will failover on Node2.
4. On Node1, run the Disk Administrator to put a signature, format the planned NTFS partition and assign a Drive Letter (Choose a drive letter that can be affected on both nodes).

5. Refresh SAN Manager LUN access control result panel to see the partitions.
6. Once partition(s) is(are) made ready for use, Allow access to the other host Node2, using SAN Manager graphical interface.
7. It is recommended to reboot Node2 when ATF is used. Applications will failover on Node1.
8. On Node2, run the Disk Administrator, to see the partitions created on Node1 and assign them the same Drive Letter than on Node1.
9. Run Cluster Administrator tool immediately to put the shared disk(s) Resource(s) under MSCS control, into a new or existing MSCS Cluster Group.
   This must be done before any access to shared disks.

From now, shared data can be setup up from Node owning the disk, (Move Group to the relevant Node if necessary).

Re–arrange applications between the 2 Nodes (if they do not have already a preferred owner Node).

Allow Access LUNs of a non–disk subsystem SAN component on NT Agent

LUNs of non–disk subsystem SAN components are automatically allowed when SAN Manager is installed (setup) on a given 'SAN Manager Agent platform'. Consequently related SAN components are made accessible for applications (backup for example) running on this SAN Manager Agent platform.

When NT SAN agent is installed, and when a new SAN component is added (plugged) to the SAN, a special operation is required in order to make the related SAN component accessible from the host.

Operation

The following procedure is to be perform on each NT SAN agent platform'; in fact on each SAN Manager Agent platform' that belongs to the zone where the SAN component was added.

The LUN Access Control must be active.

1. Open a 'Start>Programs>**Command Prompt**' window.
2. Enter the <\bin\> directory in the SAN Manager installation one.
3. Type the following command line:
   ```
   > ConfigAllUDLUN –C
   ```
   – When no denied access LUNs of non–disk subsystem SAN component is found, the following message is displayed:

   ```
   >No unknown device LUN to map
   ```
   – When denied access LUNs of a non–disk subsystem SAN component are found, a message like the following is displayed (example for an Overland LXB library):

   ```
   >Following unknown device LUN are mapped through 'Emulex LP-8000 Adapter
   0'
   >Wwn(100000E00200180E): LUN 0^QUANTUM^^DLT7000|LUN 1^QUANTUM^^DLT7000|LUN
   2^OVERLAND^^LXB

   IMPORTANT:
                       REBOOT the host andromede NOW to complete this command.
   ```
4. Exit the Command Prompt window.
5. Reboot the current SAN Manager Agent platform' when denied access LUNs of non–disk subsystem SAN component were found.

Deny Access LUNs of all non–disk subsystem SAN components on NT SAN agent

No LUN is denied access when SAN Manager is un–installed on a given SAN Manager Agent platform.

The operation described below is only needed when you plan to definitely un–installSAN Manager. This operation does not apply in case you upgrade or re–install SAN Manager.

Operation

The following procedure is to be perform on each NT SAN agent platform.

The LUN Access Control must be active.

1. Open a 'Start>Programs>**Command Prompt**' window.
2. Enter the <\bin\> directory in the NT SAN installation one.
3. Type the following command line:
   ```
   > UnConfigAllUDLUN –U
   ```
   – When no denied access LUNs of non–disk subsystem SAN component is found, the following message is displayed:

   ```
   >No unknown device LUN to un-map
   ```
   – When denied access LUNs of a non–disk subsystem SAN component are found, a message like the following is displayed (example for an Overland LXB library):

   ```
   >Following unknown device LUN are un-mapped through 'Emulex LP-8000
   Adapter 0'
   >Wwn(100000E00200180E): LUN 0^QUANTUM^^DLT7000|LUN 1^QUANTUM^^DLT7000|LUN
   2^OVERLAND^^LXB
   ```
4. Exit the Command Prompt window.

Adding a second HBA in a Windows NT host

This case applies when a host has to be upgraded in using ATF.

The initial hardware configuration is one HBA plugged in the host and SAN Manager is running. The target one is two HBAs plugged in the host, ATF installed and operational and SAN Manager running again.

1. If one or several LUNs are currently mapped,
   – note the Drive Letter of the partitions currently assigned on to the corresponding Disk#
   – deny access the related LUNs, (refer to Allow / Deny Access, on page 5-11.for details).
2. Stop (shutdown) the host.
3. Add the second HBA.

Note: Remind that the two HBAs must have the same hardware characteristics (model, revision, etc...).

4. Reboot the host.
   – At this time, the SAN Manager environment is running.
5. Continue the procedure from the step 9 of the "Global installation with ATF on page 2-7" paragraph.

Note: To recover data currently stored in the disk area of the LUN that were un–mapped in the step 1 above, assign, if any, the same Drive Letter that was previously assigned to the same partitions.

LUN Access Control on Windows NT Host

- LUN mappings information on Windows NT hosts are stored in the registry with the following organisation:
  - per fibre channel adapter (FC HBA) location (PCI bus and slot),
  - then for each FC HBA location: per subsystem port WWN.

  This organisation has the following consequences when adapters are moved within a Windows NT platform:
  - when a FC HBA is moved from a PCI slot to another, the LUN mappings associated to the initial position become ineffective and must–be replayed for the new HBA location,
  - if another FC HBA is added later into the initial slot, the LUN mappings associated with this location become active again.

This also implies that when a subsytem port (eg a DAS SP) is replaced, the LUN mappings associated with the initial SP are lost if the replacement of the subsystem port modifies its WWN, and must be replayed (see chapter "*Replacing a DAS SP*" for details).

- LUN mapping/unmapping (ie "Allow/Deny access") operations can only be performed on operational pathes (ie the link between the FC HBAs and the subsytem ports must be up). This need to be taken into account with specific attention in the case where multiple pathes between a Windows NT host and a subsystem are to be managed (especially DAS configuration with ATF).
- If several controllers of the **same DAS disk subsystem** are reachable, then the LUN mapping/unmapping operations are performed for all the controllers through which the LUNs are reachable (limited to two controllers for DAS configurations).The LUNs are displayed with the following *pv_state* in ASM GUI (window "Display LUN access control"):
  - "(**A)**vailable" on the controller that is currently used by the system (eg ATF) to reach them
  - "(**D)**efined" on the other controller.

  The same NT LUN number is assigned to each mapping of a particular FC LUN (but each controller is mapped to a different SCSI ID).

  The field "*PV name*" that appears in the "Display LUN access control" and "Subsystem LUNs" windows of ASM GUI, contains the "NT Disk #" for the path known by the system and the "NT LUN i" for the alternate path. This does not change when an *atf_trespass* (or *atf_restore*) command is issued.

  If a LUN mapping is performed after the ATF installation, a reboot is needed for ATF to take into account the new configuration (ATF versions lower than 1.1.1 must be re–installed).

  Due to the ASM SAN agent polling process, failover may be initiated outside any active operational I/O.

  For **AIX SAN agents**, the management of the *pv_state* field is a bit different:
  - If ATF is installed on the SAN agent, both pathes are displayed with *pv_state* = "**(A)**vailable" (except in the case where an explicit **rmdev hdisk** command has been manually performed).
  - If ATF is not installed, the path currently active is displayed with *pv_state* "= **(A)**vailable", whilst the other path is displayed with *pv_state* = **"(B)**ackup".

Adding a New Subsystem to the SAN

Adding a Supported and Ready Disk Subsystem

When a new disk subsystem, supported by ASM (DAS or Symmetrix subsystem), is connected to the SAN, all Windows NT hosts must be rebooted before they are allowed to

access LUNs of the new disk subsystem (ie before LUNs of the new disk subsystem can be mapped on Windows NT hosts).

Adding a Not–Supported Disk or Tape Subsystem

When a new subsytem, not supported by ASM (any type of SAN disk other than DAS or Symmetrix, or tape subsystem, or a SCSI library connected via a FC/SCSI converter), is connected to a SAN, its LUNs must be manually mapped on each Windows NT host using the following procedure:

1. The LUN Access Control must be active.
2. Open a “Start –> Programs –> Command Prompt” window.
3. Enter the \bin\ directory in the ASM SAN agent for Windows NT installation directory (default: %SystemDrive%:\Program Files\Bull\S@N.IT\)
4. Type the following command line:

   ```
   > ConfigAllUDLUN –C
   ```

   Depending on the result of the command, the operation is different:

   – When no un–mapped LUNs of non supported SAN component is found, the following message is displayed:

   ```
   >No unknown device LUN to map
   ```

   Just exit the Command Prompt window to complete the procedure.

   – When un–mapped LUNs of non supported SAN component are found, a message like the following one is displayed (example for an Overland LXB library):

   ```
   >Following unknown device LUN are mapped through 'Emulex LP-8000
   Adapter 0'
   >Wwn(100000E00200180E): LUN 0^QUANTUM^^DLT7000|LUN
   1^QUANTUM^^DLT7000|LUN 2^OVERLAND^^LXB

   IMPORTANT:

           REBOOT the host andromede NOW to complete this command.
   ```

   As indicated in the message youmust reboot the Windows NT system.

Adding a Not_Ready DAS Subsystem

Navisphere and S@N.IT! LUN Access Control

A special attention is required when using Navisphere components and ASM LUN Access Control. Navisphere supervises the disk subsystem through one Navisphere agent. Navisphere agent is configured to communicate with a disk subsystem through a path to a LUN. Once the LUN Access Control is activated on a host and no LUN is mapped, all disk subsystem LUNs are masked for this host especially LUN(s) used by Navisphere agent. Consequently, Navisphere can’t become operational; for example this occurs after the first installation of S@N.IT!.

To prevent that, it is recommended to respect the following scheme:

- For configuration without ATF, create and map one reserved LUN per host (through a *single path*) on each disk subsystem; these LUNs will be dedicated to Navisphere agents, they should not contain operational data, they can be very small, and they have not to be denied (un–mapped).
- For configuration with ATF, create and map one LUN per host (through a *dual path*) on each disk subsystem; these LUNs will allow Navisphere ATF and agent to communicate with disk subsystems. They may contain operational data.

Before using LUNs, they must have been created. This operation is generally performed once, the first time the disk subsystem is powered–on. Navisphere Supervisor is generally

used to perform this initial configuration. A Navisphere agent located on the host and a direct access to the disk subsystem through the SAN are required.

ASM provides LUN Access Control functions. These functions apply consequently when one LUN at least has been created. In addition, when the global LUN Access Control is activated, the communication between the related host and disk subsystem is closed whether LUNs exist or not.

In this context, when a new disk subsystem is to be connected to an existing SAN, there are only two possibilities to provide a direct access to the disk subsystem in order to prepare it:

- The first possibility, which is the recommended solution is to perform the preparation operation outside the SAN and to connect the disk subsystem to the SAN when at least one LUN has been created.
- The second possibility is to de-activate the LUN Access Control from the related host, to prepare the disk subsystem and to activate the LUN Access Control again. However this operation is not recommended due to the possibility for the related host to access to all LUNs seen from its HBAs during this phase.

Procedure to add a DAS

The target is to have a new disk subsystem operational through the SAN, and LUNs mapped.

- We assume that the initial state is the following one:
  - a SAN exists,
  - one or several ASM SAN agent platform(s),
  - the ASM server and ASM GUI are running,
  - Navisphere Supervisor and Navisphere agent are operational,
  - The new disk subsystem is not connected to the SAN
  - No LUN is bound in the new disk subsystem.
- The main steps of the installation are the following. Refer to *AIX SAN Manager User's Guide* for details on each operation.

1. Connect the new disk subsystem to the SAN.

   Within one minute, the new disk subsystem appears in the ASM GUI.
2. Reboot all Windows NT hosts present in the SAN.
3. Start the ASM GUI and select a host that can access the new disk subsystem. Then de-activate the LUN Access Control
4. Prepare the new disk subsystem – that is, create one LUN at least – using Navisphere.
5. Select the related host and activate the LUN Access Control again.
6. Map LUN(s) previously created on the new disk subsystem for the related host.
7. Re–configure the Navisphere agent on the related host.

Replacing a DAS SP – Impact on Windows NT LUN Access Control

This case applies when a Storage Processor (SP) is to be replaced in a DAS disk subsystem connected to a SAN managed through ASM.

The target is to have a new SP plugged on the related disk subsystem, and the LUN configuration (the previous LUN mapping) kept.

- We assume that the initial state is the following one:
  - a SAN exists,
  - one or several ASM SAN agent platform(s),
  - the ASM server and ASM GUI are running,
  - one or several LUN(s) bound on the SP that has to be replaced are mapped on one or several hosts.

The activity from the related host(s) to this SP is kept.

SPs are identified through their WWN in the system registry and LUNs are mapped regarding these WWNs. Consequently, when a new SP – with an unknown WWN – is plugged, the LUNs that were mapped on the old SP are lost. Consequently, LUN mapping has to be replayed after the new SP has been plugged.

Note: for specialists:
The LUN mapping information regarding the path to an SP that has been removed stays in the system registry. Consequently, in the case where the old SP is plugged again, the LUN mapping that was defined for this SP is re–entered. So, in this case, you have to consider and replay only the LUN mapping operations that were performed since this SP was removed. Note that this situation is unlikely to happen.

Important: It is recommended to read the following subsections ***before replacing a DAS SP***. The LUN mapping history (from the 'Log' tab in the SAN Display frame through the ASM GUI) can help you to plan the LUN mapping operations to be applied.

Replacing a SP is seen from the system as a "disks remove" operation. Consequently, after having replaced the SP, you have to map the LUNs again, and generally you must reboot the system(s).

Operations to be done depend on the number of HBA/subsystem paths that were configured before. Remind that when a dual path is found it supposes that ATF is installed.

Pay a special attention to apply strictly the procedure when ATF is active**.**

Operating without ATF

The main steps are the followings:

1. Replace the SP.

For each Windows NT host that had LUN(s) mapped on this SP:

2. Reboot the host.
3. Replay the mapping of LUNs previously mapped on the old SP.

Operating with ATF

The main steps are the followings:

1. Replace the SP.

For each Windows NT host that had LUN(s) mapped on this SP:

2. Reboot the host.
3. Un–map all LUNs previously mapped on the old SP.

When a dual path is detected, a message like the following one is displayed:

```
Un-mapping of LUN 15 succeeded on disk subsystem 1000020, type
DAS_5300, port SPA.

Un-mapping of LUN 15 FAILED on disk subsystem 1000020, type
DAS_5300.

Return code = 105

Un-mapping of LUN 15 (000F000000000000) failed on disk subsystem
3002295, type DAS_5720, port SPB, port WWN 200000601636025C
```

4. Reboot the host.
5. Replay the mapping of LUNs previously mapped on the old SP.
6. Restore the original path using the '*atf_restore*' command (refer to the "*Navisphere Application Transparent Failover (ATF) Installation and Operation for Microsoft Windows Environments*" manual).

Upgrading Firmware on a SAN Component

ASM SAN agent for Windows NT periodically sends requests to each SAN component. For this reason it is recommended to stop ASM SAN agents (stop the ‘S@N.IT! scheduler’ Windows service) before upgrading the firmware of SAN component(s).

Chapter 8. Commands (AIX Hosts only)

san_snap

Purpose

Gathers information related to SAN configuration

Syntax

/**usr**/**sbin**/**san_snap** [**–o** outputdevice] [**–d** dir] [**–w** ”problem description”]

/**usr**/**sbin**/**san_snap** [**–c**] [**–d** dir] [**–w** ”problem description”]

/**usr**/**sbin**/**san_snap** [**–r**] [**–d** dir]

/**usr**/**sbin**/**san_snap** [**–v** component]

Description

The san_snap command gathers information about SAN configuration (software level for SAN related software such as SAN Manager, Navisphere, ATF, fibre channel driver, device configuration, errlogs, traces, LUN access control, dump, unix...) and compresses the information into a tar file. The file can then be downloaded to disk or tape, or transmitted to a remote system.

The information gathered with the san_snap command may be required to identify and resolve problems.

This command is also accessible (for gathering and creation of the tar image) through the main window of the SAN Manager application.

Note: Root user authority is required to execute the snap command.

Use the san_snap –o/dev/rfd0 command to copy the compressed image to diskette.

Use the san_snap –o/dev/rmt0 command to copy the compressed image to tape.

The output of the san_snap command is written to the /tmp/sanmgr.snap directory, unless the –d option is used to specify another directory.

The san_snap command checks for available space in the /tmp/sanmgr.snap directory, the default directory for san_snap command output. You can write the output to another directory by using the –d flag. If there is not enough space to hold the san_snap command output, you must expand the file system.

Each execution of san_snap command appends information to previously created files.

Use the –r flag to remove previously gathered and saved information.

Flags

–c	Creates san_snap.tar.Z file.
–o outputdevice	Send information to removable output device (/dev/rfd0).
–d dir	Directory to put information.
–r	Remove directory (/tmp/sanmgr.snap).
–v component	Output component snap file to stdout. Current component choices are: ’dump filesys general san_mgr navisphere symmetrix install’
–w problem description	Create README file from command line.

san_saveodmCLL

Purpose:

Save and restore the ”SANmgr, San_Cl, San_Component” from/to ODM Base on an AIX SAN agent host.

Syntax:

san_saveodmCLL [**– f** file] [**–s**] [**–r**] [**–h**]

Flags

-f file	file name where the ODM base is saving. If no name is specified the name is ”/var/tmp/OdmSaveSan”.
-r	restore the base from ”file” (only when LUNs Access Control is inactive).
-s	save the base to ”file”.
-h	print the usage command.

Example:

```
san_saveodmCLL -s
san_saveodmCLL -r
```

san_trace

Purpose:

Allows you to display the contents of an AIX SAN Manager trace file. A file name may be provided as parameter. In this case, the result will be sent to the standard output. If no parameter is provided, the DISPLAY environment variable must be set and a window will appear on the screen, allowing to select the file to be displayed.

Syntax:

san_trace [filename]

Flags

filename The name of the file to be displayed on the standard output.

Example:

```
san_trace
san_trace /var/tmp/san/SANNative.ctrace
```

Display LUN Access Control Contents and State

Syntax

/usr/sbin/san_displayCLL [–h host]

Activate LUN Access Control

Syntax

/usr/sbin/san_activateCLL [–h host]

Deactivate LUN Access Control

Syntax

/usr/sbin/san_deactivateCLL [–h host]

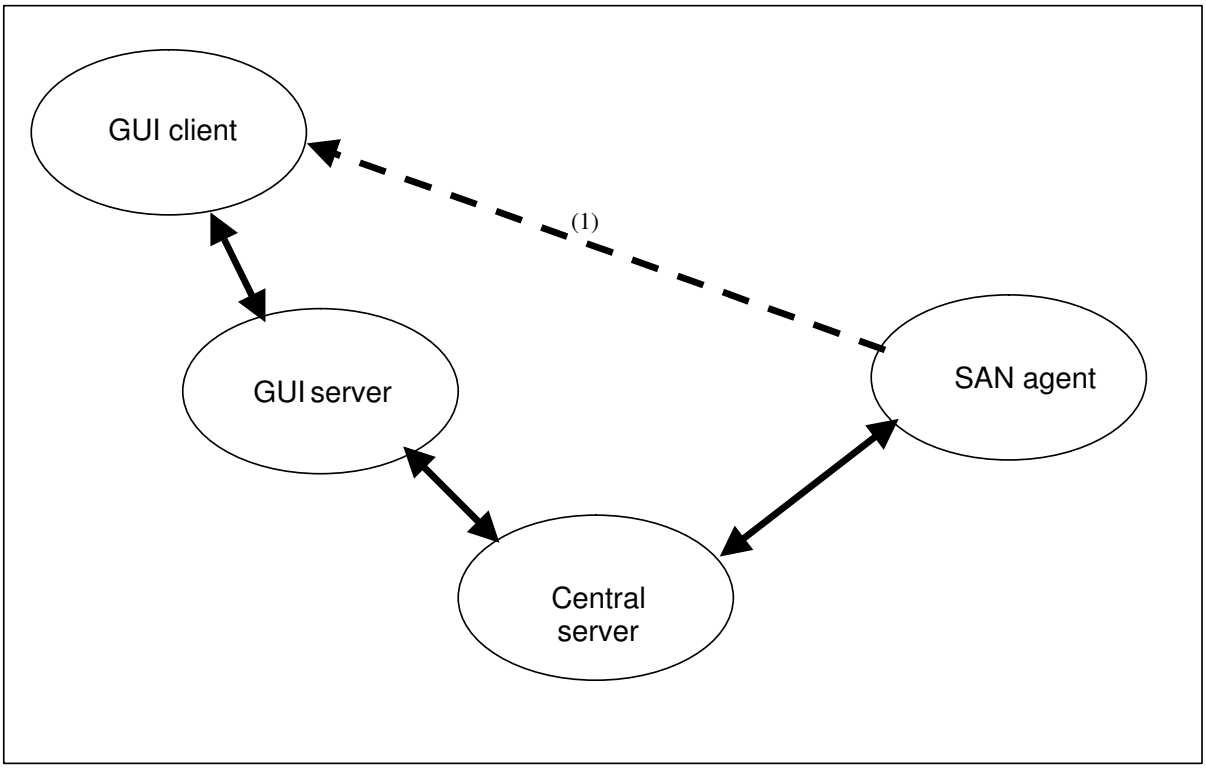
Appendix A. SAN Manager Configuration and TCP/IP Configuration

SAN Manager Configuration and TCP/IP Configuration

The different machines involved in the SAN Manager (GUI clients, GUI servers, central server, SAN agents) communicate between each other using TCP/IP connections. During a SAN Manager session, communication is established (in both directions) between:

- the GUI client and the GUI server,
- the GUI servers and the Central Server,
- the Central Server and the SAN agents,
- the SAN agents and the GUI client (when management applications such as Symmetrix Management are launched).

The following figure summarizes the communication between the SAN Manager components. Note that the same machine can contain several components, in that case the communication between those components also use TCP/IP connections but locally.



(1) only when X11 management applications (e.g. Symmetrix Management or ECC) are launched

For these connections to be established, it is necessary that:

- Both ends of the connection are linked by an IP network (either because they belong to the same IP subnetwork, or because IP routes are defined between them).
- Each end of the connection knows the IP address of the other one.

For the communication between the SAN agent and the GUI client, the IP address of the GUI client is retrieved using the DISPLAY variable either from the shell environment where the GUI is launched, or asked by the SAN Manager application.

For other communications, the IP adresses used are configured using the fields *CentralHost* and *MyHostname* in the */etc/san/SANManager.cfg* configuration file on each platform (other fields such as *CentralPort*, *LocalPort* and *ClientPort* are also involved in the communications but they should not be modified):

- CentralHost : IP name of the central server – this parameter is used locally by a GUI server or and SAN agent for their first connection to the CentralServer. It may be provided as:
  - a dotted IP address (eg ”123.123.123.123”),
  - a string (eg “ central ”) : in this case the name resolution (mapping of this string into an IP address) is done locally.
- MyHostname : IP name to be used by other machines to connect to the current one – this parameter is transmitted “ as is ” to other machines – it may be provided as:
  - a dotted IP address (eg ”123.123.123.123”),
  - a string (eg “ sanhost ”) : in this case the name resolution is performed on remote machines.

  If this field is left blank, the default is the hostname of the current machine (value returned by the *hostname* command):
  - for a *GUI server* (machine with *ClientRole=yes*), the value of *MyHostname* is transmitted to the central server that will use it to establish connections to the GUI server, so it must be set to a name which will be resolved by the central server into an IP address of the *GUI server*, accessible from the *central server*, or left blank if the hostname of the GUI server fulfills this condition.
  - for an *AIX SAN agent* (machine with *LocalRole=yes*), the value of *MyHostname* is transmitted to the *central server* that will use it to establish connections to the *AIX SAN Agent*, so it must be set to a name which will be resolved by the central server into an IP address of the *AIX SAN Agent*, accessible from the *central server*, or left blank if the hostname of the AIX SAN Agent fulfills this condition.
  - for a *central server* (machine with *CentralRole=yes*), the value of *MyHostname* is transmitted to all *GUI servers* and *AIX SAN agents*, so it must be set to a value that will be resolved on each of those machines into an IP address that allows it to access the *central server*.

    If the *central server* has several IP interfaces (and addresses), this may raise a problem as there is only one possible value of *MyHostname* that must be solved into differents IP addresses, for each *GUI server* or *SAN Agent* depending on the network they have to use to connect to the *Central server*. This can be solved in different ways:
    - by modifying on each machine the entry for the central server “ *MyHostname* “ in the */etc/hosts* files of the GUI servers and AIX SAN agents, when no DNS is used,
    - if a DNS is used, by selecting the central server “ *MyHostname* ” out with the scope of the DNS.

The following table summarizes the value of the main fields of the `/etc/san/SANManager.cfg` file depending on the role the current machine is playing in the SAN Manager.

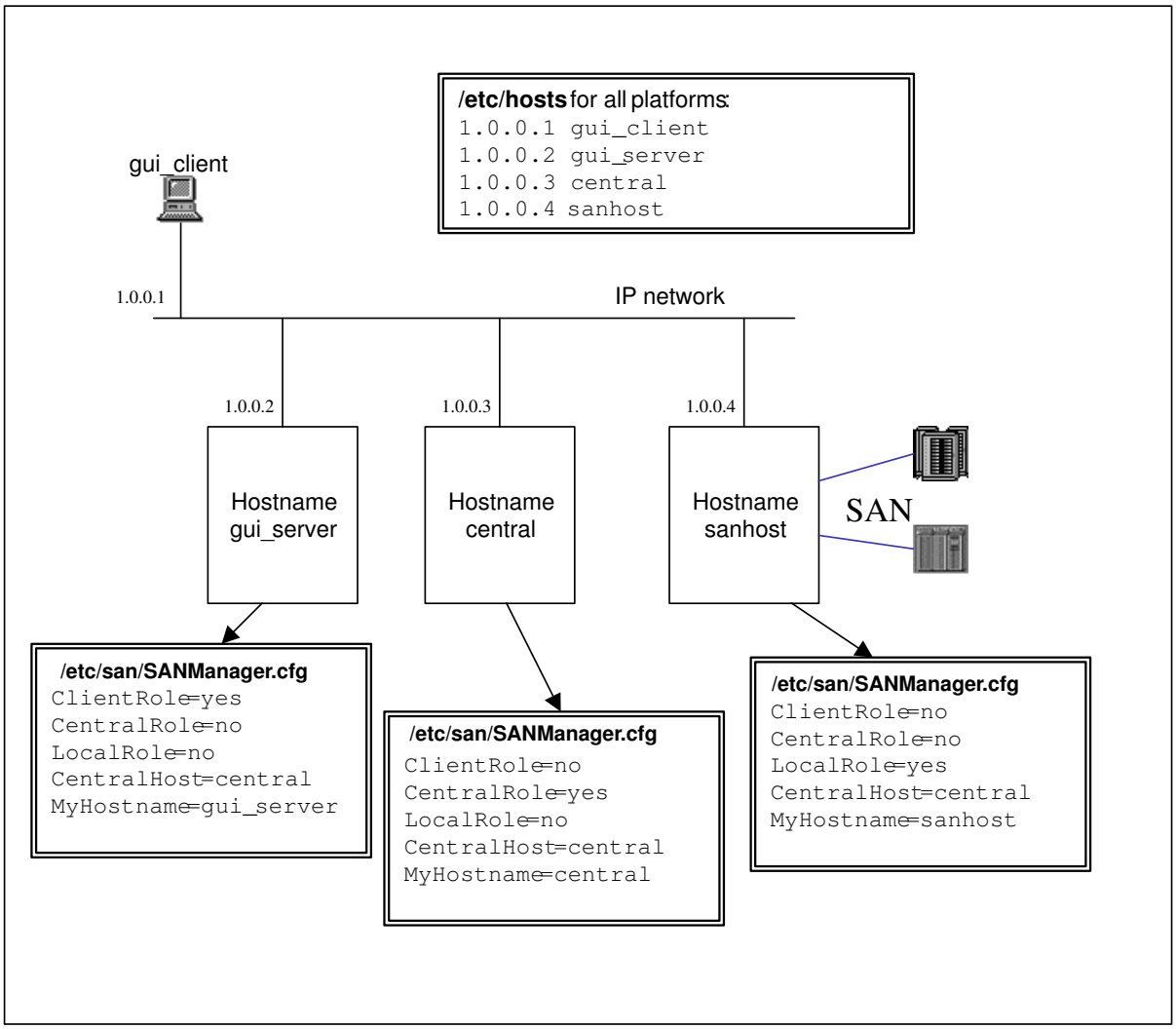
	Central Role	Local Role	Client Role	CentralHost	MyHostname	DISPLAY(2)
Central Server	Yes	No	No	Not used	IP name to be used on SAN agents and GUI servers	Not used
AIX SAN Agent	No	Yes	No	IP name of Central Server	IP name used by central server	Not used
NT SAN Agent	No	Yes	No	IP name of Central Server	IP name used by central server	Not used
GUI Server	No	No	Yes	IP name of Central Server	IP name used by Central Server	Not used
GUI Client (1)	No	No	No	No	No	Used by GUI server and SAN Agent
Central Server + GUI Server	Yes	No	Yes	Local IP name	IP name to be used on SAN agents and GUI servers (including this one)	Not used
Central Server + AIX SAN Agent	Yes	Yes	No	Local IP name	IP name to be used on SAN agents (including this one)and GUI servers	Not used
GUI server + AIX SAN Agent	No	Yes	Yes	IP name of central server	IP Name used by central server	Not used
Central Server + GUI Server + AIX SAN agent	Yes	Yes	Yes	Local IP Name	IP Name to be used on SAN agents (including this one)and GUI servers (including this one)	Not used

(1)The SAN Manager does not need to be installed on the GUI client.

(2) This parameter is not a field of the `/etc/san/SANManager.cfg` file, it is taken from the environment where the GUI client is launched or asked to the user.

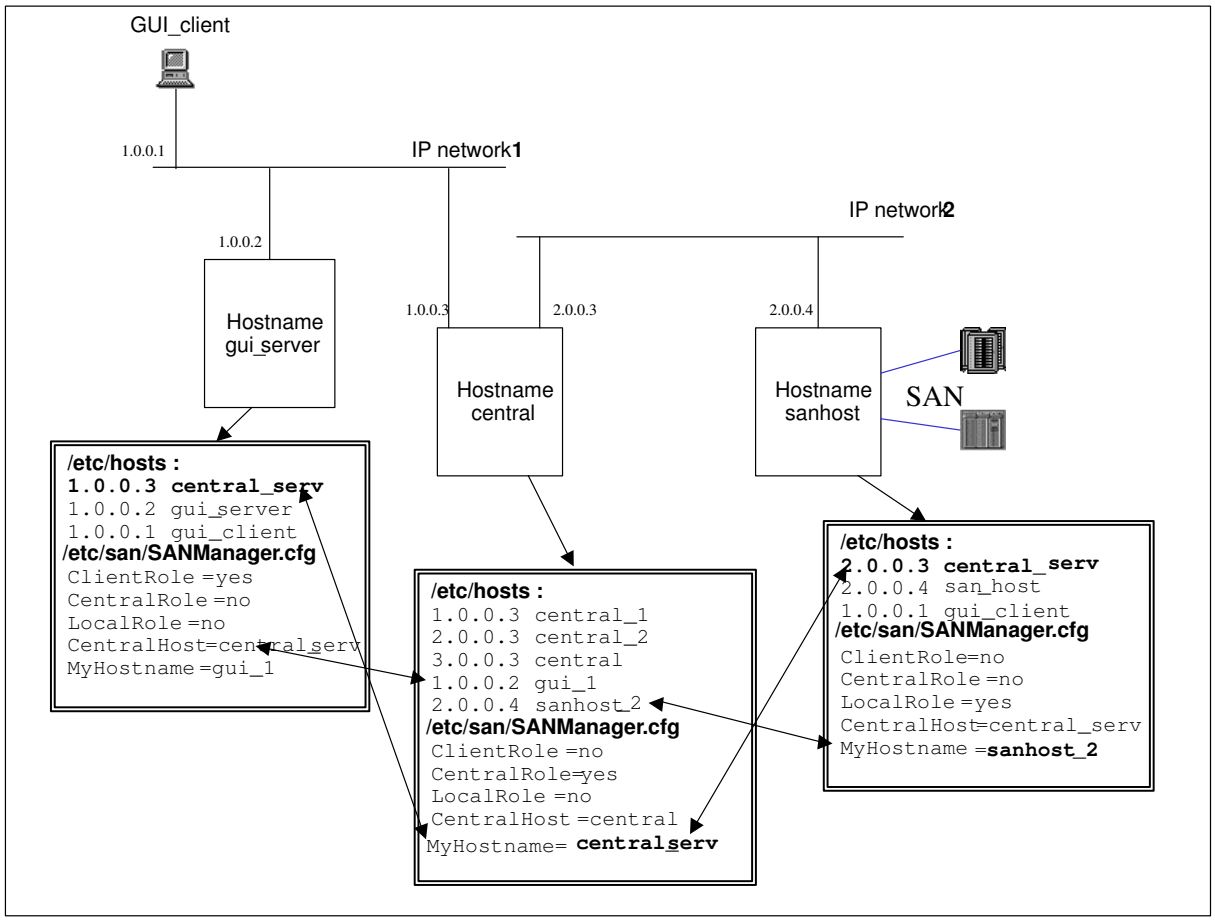
Examples

All platforms on the same IP network:



A user connected from X11 terminal (or emulation) *gui_client* will launch *wsm* on *gui_server* after setting *DISPLAY* environment variable to *gui_client :0.0*.

Central Server connected to two IP networks:



In this configuration, it is important to note that:

- On the central server machine, the value of *MyHostname* must be set to *central_serv,* because this is the name that is known on both the GUI server machine and the AIX SAN agent machine, although it is not converted to the same IP adress.
- On the GUI server (and on the AIX SAN agent), the value of *MyHostname* must be set to *gui_1* (respectively *sanhost_2*), because this is the name known by the Central Server.
- It is necessary to establish an IP route from “ sanhost ” to adress 1.0.0.1(“ GUI_client ”), otherwise it will not be possible to launch Symmetrix Management or Navisphere from an AIX SAN Manager session launched from GUI_client.

Appendix B. Example of Using SAN Manager

Example of Using SAN Manager

The following example explains which actions the administrator has to perform to configure a SAN.

Starting from scratch, all the steps are described. The SAN Manager actions used in this example are detailed later in this book.

To launch a SAN Manager session, see Starting a SAN Manager session, on Page 4-1.

SAN Configuration

The SAN configuration example consists of:

- Three hosts csmgt10, csmgt11 and csmgt12.
- A fibre DAS 5700 subsystem connected to csmgt11 (fchan2) and to csmgt10 (fchan2) through a hub.
- An EMC Symmetrix subsystem connected to csmgt11 (fchan1), to csmgt10 (fchan0) and to csmgt12 (fchan1) through a Brocade switch.
- A DAS 3500 subsystem connected to csmgt11 (fchan0) through a point to point connection.

The following figure illustrates this configuration.

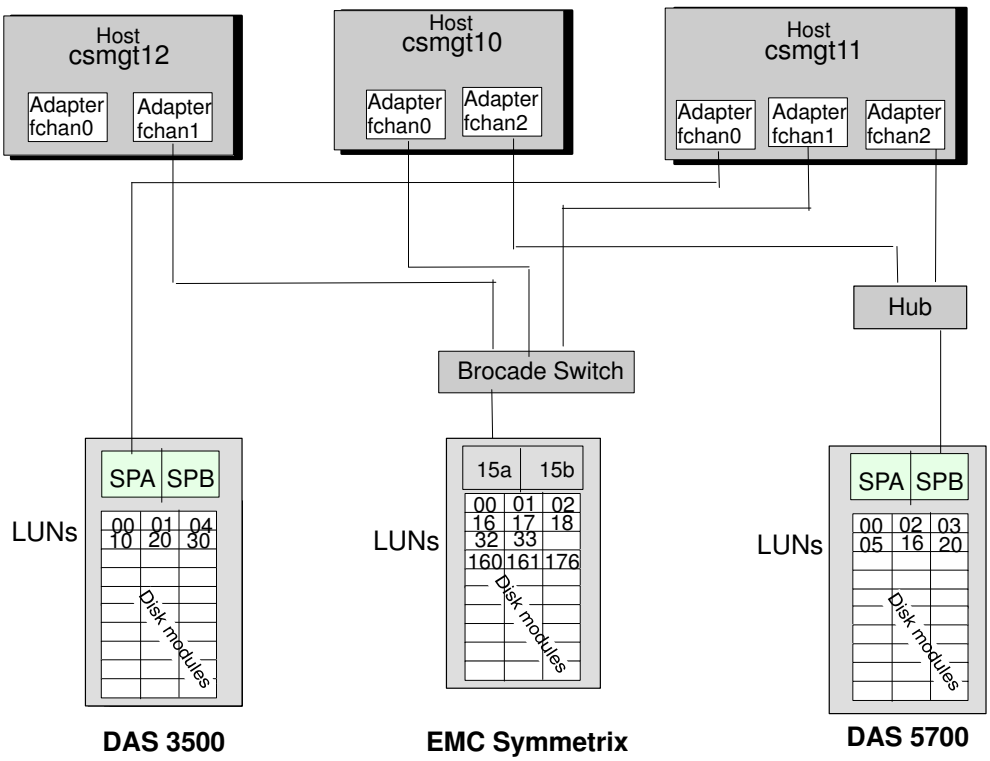


Figure 23. SAN Configuration example, original SAN view

This configuration may be displayed graphically by the SAN Manager using Display Graphical Topology, see page 4-1.

SAN Objective View

In order to share the available storage resources with other hosts, we will limit the visibility and accessibility to the configuration as described in the table below.

Hosts	fchan	DAS 5700	EMC Symme-trix	DAS 3500
csmgt10	fchan0		LUN 18, LUN 32, LUN 33	
	fchan2	LUN 0, LUN 5		
csmgt11	fchan0			LUN 1, LUN 10, LUN 30
	fchan1		LUN 16, LUN 17	
	fchan2	LUN 2, LUN 3		

Table 1. SAN Manager visibility and accessibility example.

Configuration Procedure

The following procedure describes all the actions to be done to reach the SAN objective view.

Manage Domains

In order to limit SAN view to csmgt10 and csmgt11, we will create a domain (doc) which gathers these two hosts (refer to Manage Domains, on Page 5-4).

1. create a new domain doc
2. select the domain doc
3. select add a host action
4. select csmgt10 and csmgt11
5. valid

Select a Domain

Use this action to display in the main window, only the hosts belonging to the doc domain (see Select a Domain, on Page 5-6).

LUNs Access Control

Now we limit the visibilty to the LUNs indicated in the Table 1.

EMC

1. Select the EMC on the main window.
2. Display the subsystem LUNs window (refer to Display Subsystem LUNs, on Page 5-11).
   - Select the host csmgt10 and the fchan0.
   - Select the LUNs 18, 32 and 33.
   - Allow access.
3. Idem for csmgt11 selecting on fchan1 the LUNs 16 and 17. Allow access.

DAS5700

1. Select the DAS5700 on the main window.
2. Display the subsystem LUNs window (refer to Display Subsystem LUNs).
   - Select the host csmgt10 and the fchan2.
   - Select the LUNs 00 and 05.

– Allow access.

3. Idem for csmgt11 selecting on fchan2 the LUNs 02 and 03. Allow access.

DAS3500

1. Select the DAS3500 on the main window.
2. Display the subsystem LUNs window (refer to Display Subsystem LUNs).
   – Select the host csmgt11 and the fchan0.
   – Select the LUNs 01, 10 and 30.
   – Allow access.

Activate LUN Access Control

Perform, in order to have only the LUNs present in the LUNs Access Control accessible.

A reboot of the host must be done to make the LUNs Access Control 'active'.

After the reboot, the SAN visibility is like the following:

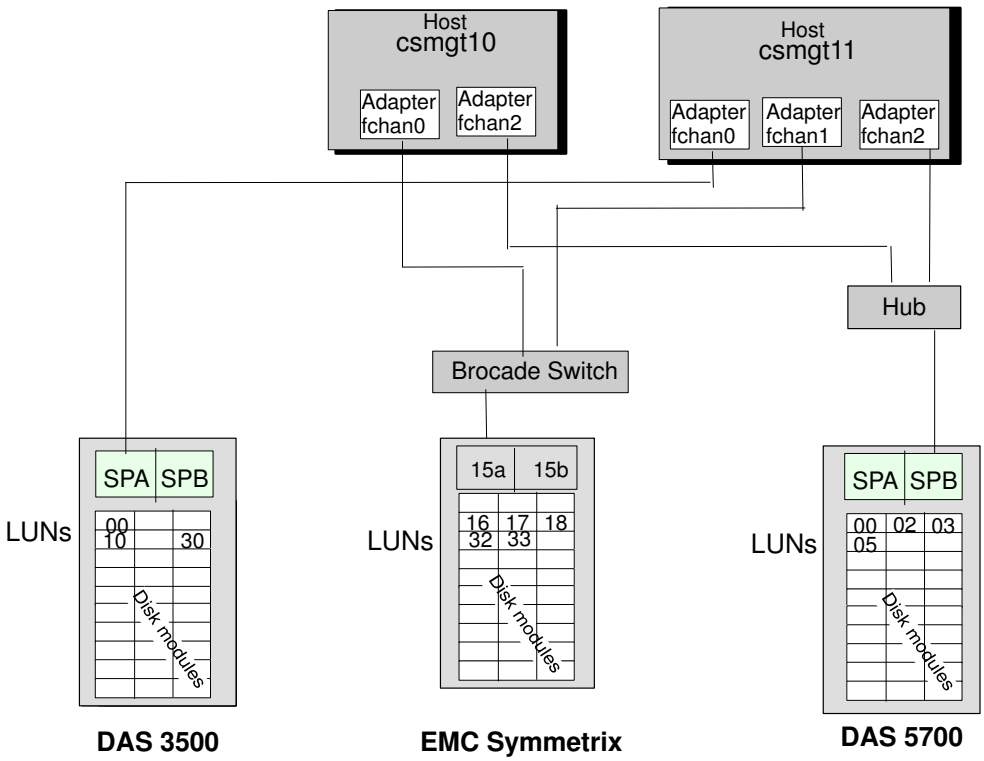


Figure 24. SAN Configuration example, final SAN view

Appendix C. Reporting Procedure on a Windows NT SAN Agent

Reporting Procedure on a Windows NT SAN Agent

When a trouble occurs, please respect the procedure described below to report dump information to your support representative.

Note: Do not perform any administration or maintenance operations before taking a snap (dump) of the current state.

Perform successively the following operations:

1. Take a snap.
2. Describe the trouble.
3. Send the information to support

Take a snap

The following procedure is to be performed on each Windows SAN agent platform:

Start the **snap.bat** command from the directory:
<*ASM SAN agent for Windows NT installation path\bin*>

The following messages are displayed during the snap processing:

```
Remove snap<HOSTNAME> directory
Retrieve system information
Retrieve registry information
Retrieve event log information
Retrieve S@N.IT! information
New snap information takes place in snap<HOSTNAME> directory
Press any key to continue . . .
```

The dump information is located in the directory
< *ASM SAN agent for Windows NT installation path \snap<HOSTNAME*>
(default installation_path <`C:\Program Files\Bull\S@N.IT\`>).

Describe the trouble

1. Using your favorite editor, write a "reporting paper" that will summarize your visibility of the trouble. Especially:
   - The using context: Hardware topology, state of the leds on each SAN component involved (HBAs, interconnect and ports, subsystems and SPs).
   - Your own external visibility and your understanding of the trouble.
   - The last external events that occurred. Pay particular attention to the last hardware handling and/or administrative operations performed through the miscellaneous administration interfaces.
   - Any information and complementary descriptions that will help the support team to determine the source of the trouble.
2. Archive the "reporting paper".

Send to support:

Call your support representative and send him archive files, that is:

- For each host platform the content of the <*S@N.IT!_installation_path**snap*<*HOSTNAME*\> directory.
- The reporting paper file.

Setting the debug mode

Upon maintenance people request, debugging traces may be set as follows:

1. Stop the ‘S@N.IT! scheduler’ NT service on the host(s) you want setting trace
2. Run your favorite text editor on the S@N.IT! configuration file <`SANManager.cfg`> located in the S@N.IT! installation directory.
3. Search for the “`TraceDevice`“ token and Set it to the value “2”.
4. Save the S@N.IT! configuration file (text format only) and exit the editor.
5. Re–start the ‘S@N.IT! scheduler’ NT service

Glossary

This glossary contains abbreviations, key–words and phrases that can be found in the SAN Manager documentation.

AIX
Advanced Interactive eXecutive. IBM UNIX™ operating system derived from AT&T UNIX™ System V.

ASM
AIX SAN Manager

ATF
Automatic Transparent Failover

CD
Channel Director

DAE (disk array enclosure)
A storage device that includes an enclosure, up to 10 or 30 disk modules (depending on model), one or two Fibre Channel LCCs, and one or two power supplies.

DPE (disk array processor enclosure)
A storage device that includes an enclosure, up to 10 disk modules, one or two SPs, one or two Fibre Channel LCCs, and one or two power supplies. A DPE can support up to 11 DAEs (each with up to 10 disk modules) in addition to its own 10 disk modules, for a total of 120 disk modules. You can attach a DPE to one or more servers or external hubs in any of many different configurations.

Fabric
The term fabric is used to refer to a set of interconnected switches, even if the set is limited to a single switch.

FC–AL (Fibre Channel Arbitrated Loop)
An arrangement of Fibre Channel stations such that messages pass from one to the next in a ring.

FCP
Fibre Channel Protocol for SCSI

JBOD (just a bunch of disks)
Another name for DAE (Disk Array Enclosure).

LCC
Link Control Card.

LPP
Licensed Program Product.

LUN (logical unit)
One or more disk modules (each having a head assembly and spindle) bound into a group — usually a RAID group. The operating system sees the LUN, which includes one or more disk modules, as one contiguous span of disk space.

MP
Multi-processor.

MSCS
Microsoft Cluster Server. High Availability in windows NT: distributed architecture, DB server and CI must be on a separate node.

NetLS
Network License System.

NLS
National Language Support.

OPP
Optional Program Product.

PCI
Peripheral Component Interconnect (Bus).

SAN (Storage Area Network)
A high speed network that establishes a direct connection between storage elements and servers or clients.

SP (storage processor)
A printed-circuit board with memory modules and control logic that manages the storage-system I/O between the server FC adapter and the disk modules. The SP in a DPE storage system sends the multiplexed fibre channel loop traffic through a link control card (LCC) to the disk units. For higher availability and greater flexibility, a DPE can use a second SP.

WebSM
Web–based System Manager.

Index

Vos remarques sur ce document / Technical publication remark form

Titre / Title : Bull SAN Manager User's Guide

Nº Reférence / Reference Nº : 86 A2 86KX 05

Daté / Dated : April 2001

ERREURS DETECTEES / ERRORS IN PUBLICATION

AMELIORATIONS SUGGEREES / SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Vos remarques et suggestions seront examinées attentivement.
Si vous désirez une réponse écrite, veuillez indiquer ci-après votre adresse postale complète.

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.
If you require a written reply, please furnish your complete mailing address below.

NOM / NAME : _____ Date : _____

SOCIETE / COMPANY : _____

ADRESSE / ADDRESS : _____

_____

Remettez cet imprimé à un responsable BULL ou envoyez-le directement à :

Please give this technical publication remark form to your BULL representative or mail to:

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

Technical Publications Ordering Form

Bon de Commande de Documents Techniques

To order additional publications, please fill up a copy of this form and send it via mail to:
Pour commander des documents techniques, remplissez une copie de ce formulaire et envoyez-la à :

BULL CEDOC
ATTN / MME DUMOULIN
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

Managers / Gestionnaires :
Mrs. / Mme : **C. DUMOULIN** +33 (0) 2 41 73 76 65
Mr. / M : **L. CHERUBIN** +33 (0) 2 41 73 63 96

FAX : +33 (0) 2 41 73 60 19
E–Mail / Courrier Electronique : srv.Cedoc@franp.bull.fr

Or visit our web sites at: / Ou visitez nos sites web à:

http://www.logistics.bull.net/cedoc

http://www-frec.bull.com http://www.bull.com

CEDOC Reference # Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
[_ _] : **no revision number means latest revision** / pas de numéro de révision signifie révision la plus récente					

NOM / NAME : ______________________________ Date : __________

SOCIETE / COMPANY : ______________________________

ADRESSE / ADDRESS : ______________________________

____

PHONE / TELEPHONE : ____________________ FAX : ____________________

E–MAIL : ______________________________

For Bull Subsidiaries / Pour les Filiales Bull :

Identification: ______________________________

For Bull Affiliated Customers / Pour les Clients Affiliés Bull :

Customer Code / Code Client : ______________________________

For Bull Internal Customers / Pour les Clients Internes Bull :

Budgetary Section / Section Budgétaire : ______________________________

For Others / Pour les Autres :

Please ask your Bull representative. / Merci de demander à votre contact Bull.

PLACE BAR CODE IN LOWER LEFT CORNER

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

ORDER REFERENCE
86 A2 86KX 05

Bull

Utiliser les marques de découpe pour obtenir les étiquettes.
Use the cut marks to get the labels.

AIX
SAN Manager
User's Guide

86 A2 86KX 05

AIX
SAN Manager
User's Guide

86 A2 86KX 05

AIX
SAN Manager
User's Guide

86 A2 86KX 05