VERITAS™

VERITAS SANPoint Control™ QuickStart 4.0

SANPoint Control QuickStart Installation and Configuration Guide

Solaris

N09883F

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

VERITAS Copyright

Copyright © 2000–2004 VERITAS Software Corporation. All rights reserved. VERITAS, VERITAS Software, the VERITAS logo, VERITAS SANPoint Control QuickStart, and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo, and SANPoint Control QuickStart Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies.

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650–527–8000 Fax 650–527–2901
www.veritas.com

Third-Party Copyrights

ACE and TAO

ACE and TAO are copyrighted by Douglas C. Schmidt and his research group at Washington University and University of California, Irvine, Copyright 1993-2002, all rights reserved.

Apache

Apache Jakarta Lucene. Copyright © 2000 The Apache Software Foundation. All rights reserved. This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Apache Xerces-C XML parser Copyright © 1999-2001 The Apache Software Foundation. All rights reserved. This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

XML4C Copyright © 1999-2001 The Apache Software Foundation. All rights reserved. This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Centura Software Corporation

Raima and Centura are trademarks of Centura Software Corporation in the United States and other countries. Some software products marketed by Centura Software Corporation and its distributors contain proprietary software components of other software vendors. Copyright © 2000 Centura Software Corporation. All rights reserved.

GRAPH EDITOR TOOLKIT

GRAPH EDITOR TOOLKIT Copyright © 1992–1999 Tom Sawyer Software, Berkeley, California. All rights reserved.

International Components for Unicode (ICU)

International Components for Unicode (ICU), Version 2.0, Copyright (c) 1995-2002 International Business Machines Corporation and others. All rights reserved.

Net-SNMP

Copyright 1989, 1991, 1992 by Carnegie Mellon University; Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California All Rights Reserved; Copyright 2001-2002, Networks Associates Technology, Inc.All rights reserved; Copyright 2001-2002, Cambridge Broadband Ltd. All rights reserved.

OpenSSL Organization

This product includes software developed by the OpenSSLProject for use in the OpenSSL Toolkit (http://www.openssl.org/).

PERL KIT

PERL KIT, Versions 5.005 and 5.6.1 Copyright 1989-2000, Larry Wall. All rights reserved.

STLport 4.5

STLport 4.5 Copyright © 1999-2000 Boris Fomitchev; Copyright © 1994 Hewlett-Packard Company; Copyright © 1996-1997 Silicon Graphics Computer Systems, Inc.; Copyright © 1997 Moscow Center for SPARC Technology. Full text of the License agreement is available at http://www.stlport.org/doc/license.html

Contents

Tasks at a Glance . . . . . **ix**

Preface . . . . . **xi**

Overview of SANPoint Control QuickStart 4.0 xii

Features in the SANPoint Control Product Family xiii

Upgrading from SANPoint Control QuickStart xiv

What's In This Manual? xv

Catalog of Product Manuals xvi

Related Resources xvii

Conventions xviii

Getting Help xx

Understanding How to Troubleshoot SANPoint Control QuickStart xxi

Contacting VERITAS xxii

Chapter 1. SANPoint Control QuickStart Installation Overview **1**

Documents You Need To Plan Your Installation 2

What Is a Typical Installation Configuration for SANPoint Control QuickStart? 3

Multi-Fabric SANs 3

Choosing SANPoint Control QuickStart Hosts 5

Choosing a SANPoint Control QuickStart Server Host 5

Choosing a SANPoint Control QuickStart Agent Host 5

Choosing a VERITAS Enterprise Administrator (VEA) Console Host 6

Chapter 2. Device and Application Interoperability Requirement Checklists 7
Interoperability Requirements for Applications 9
VERITAS Volume Manager Requirements 10
VERITAS NetBackup Requirements 11
VERITAS Cluster Server Requirements 12
IBM DB2 EE and EEE Requirements 13
Oracle Requirements 14
Interoperability Requirements for Switches 15
Brocade Switch Requirements 16
Cisco Switch Requirements 19
INRANGE Switch Requirements 21
McDATA Switch Requirements 23
QLogic Switch Requirements 25
Firewall Requirements 27
Interoperability Requirements for HBAs 29
Emulex HBA Requirements 30
JNI HBA Requirements 32
QLogic HBA Requirements 34
Interoperability Requirements for Bridges and Routers 36
Cisco Router Requirements 37
Chaparral Bridge Requirements 38
Crossroads Bridge Requirements 39
Hewlett-Packard Bridge Requirements 40

Chapter 3. Installing SANPoint Control QuickStart 41
Installing the SANPoint Control QuickStart Server 42
Installing the SANPoint Control QuickStart Agent 44
Installing the VERITAS Enterprise Administrator (VEA) Console 46

Chapter 4. Getting Basic Configuration Data About Your SAN 49
Understanding the SANPoint Control QuickStart Configuration Utility 51

Running the SANPoint Control QuickStart Configuration Utility 53
Viewing the SANPoint Control QuickStart Configuration Utility Report 57
Manually Updating the Compatibility List 59

Chapter 5. Configuring SANPoint Control QuickStart Discovery 61
Configuring SANPoint Control QuickStart Discovery Overview 63
Direct Attached Storage (DAS) Discovery Considerations 65
Configuring the Server for Agent Discovery 66
Configuring the Server for Cisco MDS Switch Discovery 68
Configuring the Server for Switch SNMP Discovery 71
Adding or Modifying Brocade Switch Credentials 72
Configuring the Server for Bridge and Router Discovery 74
Configuring the Oracle Explorer 75
Disabling CT Passthru 77
Configuring Discovery When Removing SAN Devices 78
Removing Cisco MDS Switches from Discovery 79
Removing Switches Discovered With the SNMP Explorer 80
Removing Bridges and Routers from Discovery 81

Chapter 6. Running SANPoint Control QuickStart 83
Stopping and Starting SANPoint Control QuickStart 84
Connecting to the SANPoint Control QuickStart Server 85

Chapter 7. Uninstalling SANPoint Control QuickStart 87
Uninstalling SANPoint Control QuickStart 88
Uninstalling the VERITAS Enterprise Administrator (VEA) Console 90

Appendix A. Command and Configuration File Reference 91
Commands and Configuration Files Locator 92
spcconfig 93
vxDB2 98

vxOra 100
sal.conf 102
vxsal 131
vxsald 133

Appendix B. Troubleshooting 135
Installation Issues 136
Configuration Issues 137
Oracle Discovery Issues 140
VERITAS NetBackup Discovery Issues 141
VERITAS Volume Manager Discovery Issues 142
VERITAS Cluster Server Discovery Issues 143
Performance Issues 144
Issues When Starting and Stopping SANPoint Control QuickStart Components . . 145
Connection Issues 146

Appendix C. SANPoint Control QuickStart and Dependency Installation Packages 147

Index 149

Tasks at a Glance

Chapter 1. SANPoint Control QuickStart Installation Overview 1

Chapter 2. Device and Application Interoperability Requirement Checklists 7

Chapter 3. Installing SANPoint Control QuickStart 41

To install the SANPoint Control QuickStart Server 42

To install the SANPoint Control QuickStart Agent 44

To install the VEA Console on Solaris 46

To install the VEA Console on Windows 47

Chapter 4. Getting Basic Configuration Data About Your SAN 49

To run the SANPoint Control QuickStart Configuration Utility 53

To view the SANPoint Control QuickStart Configuration Utility report 57

To manually update the compatibility list 59

Chapter 5. Configuring SANPoint Control QuickStart Discovery 61

To configure SANPoint Control QuickStart discovery 63

To configure the QuickStart Server for QuickStart Agent host discovery 66

To configure the QuickStart Server for Cisco MDS switch discovery 68

To configure the QuickStart Server for SNMP discovery 71

To add or modify Brocade switch credentials on a SANPoint Control QuickStart Server host 72

To configure the QuickStart Server for bridge and router discovery 74

To configure the SANPoint Control QuickStart Oracle explorer 75

To disable the MGEX explorer from using in-band operations 77

To reconfigure the QuickStart Server for discovery when SAN devices are removed 78
To remove Cisco MDS switches from discovery 79
To remove switches from SNMP explorer discovery 80
To remove bridges and routers from discovery 81

Chapter 6. Running SANPoint Control QuickStart 83
To stop or to restart SANPoint Control QuickStart 84
To connect to the SANPoint Control QuickStart Server on Solaris 85
To connect to the SANPoint Control QuickStart Server on Windows 86

Chapter 7. Uninstalling SANPoint Control QuickStart 87
To uninstall SANPoint Control QuickStart 88
To uninstall the VEA Console on Solaris 90
To uninstall the VEA Console on Windows 90

Preface

Welcome to the SANPoint Control QuickStart 4.0 documentation set. The manuals and online help included with SANPoint Control QuickStart will show you how you can use the product to view, monitor, and manage your SAN.

The information in this Preface helps you find what you need in the product documentation and tells you how to get help when you need it.

This section includes the following topics:

"Overview of SANPoint Control QuickStart 4.0" on page xii

"Features in the SANPoint Control Product Family" on page xiii

"Upgrading from SANPoint Control QuickStart" on page xiv

"What's In This Manual?" on page xv

"Catalog of Product Manuals" on page xvi

"Related Resources" on page xvii

"Conventions" on page xviii

"Getting Help" on page xx

"Understanding How to Troubleshoot SANPoint Control QuickStart" on page xxi

"Contacting VERITAS" on page xxii

Overview of SANPoint Control QuickStart 4.0

SANPoint Control QuickStart provides automatic, accurate discovery and visualization of SAN devices. For discovered devices, SANPoint Control QuickStart provides detailed attributes and connectivity information, thus eliminating the need for manually tracking SAN assets.

SANPoint Control QuickStart is a VERITAS Enterprise Administrator (VEA) extension. Its graphical user interface displays within VEA and includes a graphical Topology Map that exposes the interrelationships between your SAN devices. SANPoint Control QuickStart provides the broad view of the entire storage network that you require while at the same time giving you the ability to drill down to specific information like data paths and resource relationships.

Features in the SANPoint Control Product Family

The following table provides a high-level summary of the features available in SANPoint Control QuickStart and its parent product, SANPoint Control.

Comparison of SANPoint Control Product Family Features

Task	QuickStart	Full Product
Discover and visualize SAN devices and meta-objects, such as fabrics and virtual fabrics	✓	✓
View graphical representation of SAN topology	✓	✓
Create groups to meet quality-of-service requirements	✓	✓
View and export inventory reports	✓	✓
Create device enclosures and hosts for partially-discovered objects	✓	✓
Launch VERITAS Volume Manager in-context from within Console	✓	✓
Launch other VERITAS and supported third-party applications in-context from within Console		✓
Issue commands using the command-line interface		✓
Control access to SAN resources through zone management		✓
Create policies to monitor and report on SAN performance and utilization		✓
Use LUN security to manage hosts' access to LUNs within arrays		✓
Manage arrays, including binding and masking LUNs		✓
Manage fabrics and virtual fabrics		✓
Perform trace routes to identify potential bottlenecks that prevent optimal SAN performance		✓
Create customized attributes and wire connection information		✓
Analyze storage consumption to discern storage trends and needs		✓

Upgrading from SANPoint Control QuickStart

If you would like to upgrade from SANPoint Control QuickStart to its parent product, which contains additional features for managing and monitoring your SAN, contact your VERITAS sales representative.

What's In This Manual?

The *SANPoint Control QuickStart Installation and Configuration Guide* contains information about configuring SAN devices and applications prior to installing SANPoint Control QuickStart. The manual also contains information about how to install, run, and uninstall SANPoint Control QuickStart components.

This manual is organized as follows:

Chapter 1, "SANPoint Control QuickStart Installation Overview," lists the documents you need to plan your installation, describes a typical SANPoint Control QuickStart installation, and helps you decide on which hosts to install the various SANPoint Control QuickStart components.

Chapter 2,"Device and Application Interoperability Requirement Checklists," summarizes pre-install SAN setup and configuration requirements for devices and applications, as well as post-install SANPoint Control QuickStart configuration tasks.

Chapter 3,"Installing SANPoint Control QuickStart," describes how to install SANPoint Control QuickStart components.

Chapter 4,"Getting Basic Configuration Data About Your SAN," introduces the SANPoint Control QuickStart Configuration Utility and how to use it to identify configuration problems on your SAN.

Chapter 5,"Configuring SANPoint Control QuickStart Discovery," gives step-by-step instructions for configuring SANPoint Control QuickStart for device and application discovery.

Chapter 6,"Running SANPoint Control QuickStart," describes how to start and to stop SANPoint Control QuickStart components.

Chapter 7,"Uninstalling SANPoint Control QuickStart," explains how to remove SANPoint Control QuickStart components.

Appendix A,"Command and Configuration File Reference," lists SANPoint Control QuickStart commands and configuration files.

Appendix B,"Troubleshooting," explains how to handle issues related to installing, configuring, and operating SANPoint Control QuickStart. It also provides help for solving problems related to system performance.

Appendix C,"SANPoint Control QuickStart and Dependency Installation Packages," lists SANPoint Control QuickStart installation packages and the additional packages on which QuickStart is dependent.

Catalog of Product Manuals

Portable Document Format (PDF) versions of SANPoint Control QuickStart manuals are installed by default in `/opt/VRTSspqdc`.

The following manuals ship with SANPoint Control QuickStart.

Manuals in the SANPoint Control QuickStart Documentation Set

Manual	Abbreviated Title	Filename
SANPoint Control QuickStart Installation and Configuration Guide	*Install*	`spcqs_install_icg.pdf`
SANPoint Control QuickStart Overview Guide	*Overview*	`spcqs_overview.pdf`
SANPoint Control QuickStart Release Notes	*RelNotes*	`spcqs_notes.pdf`
VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List	*HCL*	`spcqs_suptmx.pdf`

Related Resources

In addition to the documentation included with SANPoint Control QuickStart, the following documentation provides information about Storage Foundation and the VERITAS Enterprise Administrator (VEA) Console:

- *Storage Solutions Installation Guide*—provides important information about how to license, install, and get support for Storage Foundation products . You should read this guide before you install SANPoint Control QuickStart. The document is available in print and in PDF format (`storage_solutions_ig.pdf`) at the top level of the VERITAS Storage Solutions software disc 2.
- VERITAS Enterprise Administrator (VEA) Console online help—provides basic information about how to use the VEA Console.
- VERITAS Volume Manager online help—provides information about how to use VERITAS Volume Manager to manage volumes, disks, and disk groups.
- VERITAS File System online help—provides information about how to use VERITAS File System to perform basic file system operations, such as adding a file system to a volume or mounting a file system.
- Storage Solutions documentation disc—a disc that enables you to search across all Storage Foundation product documentation. For more information on how to use the searchable documentation disc, see the *Storage Solutions Installation Guide*.

Conventions

The following conventions apply throughout the documentation set.

Screen Shots

The majority of screen shots in the manuals and help were taken on Windows systems. Unless otherwise noted, the application and its GUI are the same across platforms. For cases where the application or GUI is different on UNIX, a UNIX screen shot has been included as well.

Typographical Conventions

Here are the typographical conventions used throughout the manuals:

Conventions

Convention	Description
GUI Font	Used to depict graphical user interface (GUI) objects, such as fields, listboxes, menu commands, and so on. For example: Enter your password in the **Password** field.
Italics	Used for placeholder text, book titles, new terms, or emphasis. Replace placeholder text with your specific text. For example: Replace *filename* with the name of your file. Do *not* use file names that contain spaces.
`Code`	Used to show what commands you need to type, to identify pathnames where files are located, and to distinguish system or application text that is displayed to you or that is part of a code example.
Key+Key	Used to show that you must hold down the first key while pressing the second key. For example: Ctrl+S means hold down the Ctrl key while you press S.

You should use the appropriate conventions for your platform. For example, when specifying a path, use backslashes on Microsoft Windows and slashes on UNIX. Significant differences between the platforms are noted in the text.

Tips, notes, and cautions are used to emphasize information. The following samples describe when each is used.

Tip Used for nice-to-know information, like a shortcut.

Note Used for important information that you should know, but that shouldn't cause any damage to your data or your system if you choose to ignore it.

Caution Used for information that will prevent a problem. Ignore a caution at your own risk.

Getting Help

You can access SANPoint Control QuickStart online help from within the VERITAS Enterprise Administrator (VEA) Console. Within the VEA Console, select **Help > Contents**. In the help viewer's table of contents, expand the SANPoint Control QuickStart help set.

Manual pages for SANPoint Control QuickStart are installed by default in `/opt/VRTSspqmn`.

Understanding How to Troubleshoot SANPoint Control QuickStart

If an issue arises while you are using SANPoint Control QuickStart, we recommend that you follow these steps:

1. Use the manuals' troubleshooting appendixes to see if you can find the solution to your problem.

2. If your problem is not listed in the troubleshooting appendixes, check the TechNotes on the VERITAS Support Web site at http://support.veritas.com.

3. If you still can't solve your problem, you can use the `VRTSexplorer` Diagnostic Program. Do the following:

   a. Run `VRTSexplorer` as root. `VRTSexplorer`, also known as vxexplorer and vxexplore, is a tool provided by VERITAS Software Corporation that, when executed on a UNIX system, gathers some of the information that may be needed by VERITAS Technical Support to troubleshoot a problem.

   Note If `VRTSexplorer` is not already installed, install it from the CD-ROM. Under the `support` directory are directories for each supported platform. In each directory is a `README.VRTSspt` file with installation instructions.

   b. Transfer the resulting file to the VERITAS Support FTP server when asked.

   c. Call VERITAS Technical Support (see "Contacting VERITAS" on page xxii).

Contacting VERITAS

For assistance with any of the VERITAS products, contact VERITAS Technical Support:

- U.S. and Canadian Customers: 1-800-342-0652
- International: +1-650-527-8555
- Email: support@veritas.com

For license information:

- Phone: 1-650-527-0300
- Email: license@veritas.com
- Fax: 1-650-527-0952

For software updates:

- Email: swupdate@veritas.com

For information on purchasing VERITAS products:

- Phone: 1-800-258-UNIX (1-800-258-8649) or 1-650-527-8000
- Email: vx-sales@veritas.com

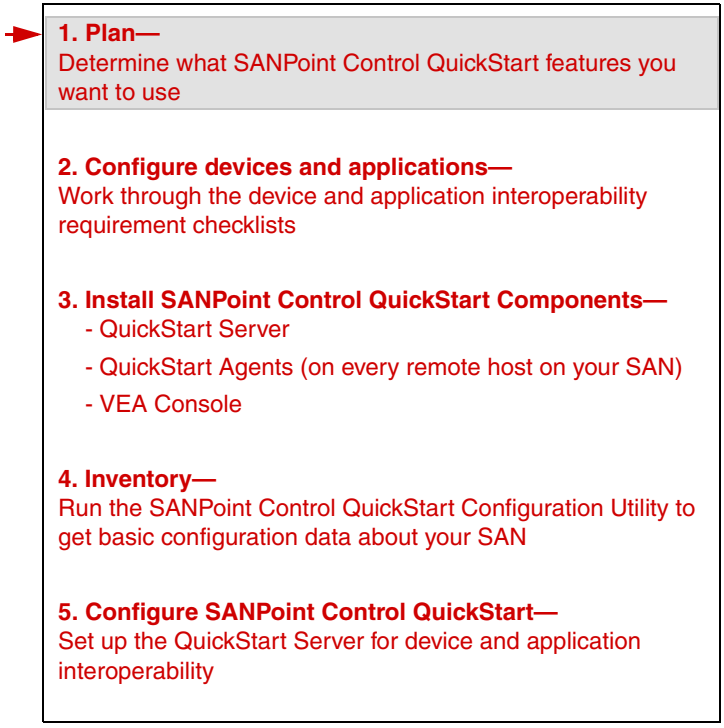
For additional information about VERITAS and VERITAS products, visit the Web site at http://www.veritas.com.

For software updates and additional technical support information, such as TechNotes, product alerts, and hardware and software compatibility lists, visit the VERITAS Technical Support Web site at: http://support.veritas.com.

SANPoint Control QuickStart Installation Overview 1

This section describes planning steps you need to take before configuring your SAN and installing SANPoint Control QuickStart.

SANPoint Control QuickStart Installation and Configuration Flowchart



This section contains the following topics:

"Documents You Need To Plan Your Installation" on page 2

"What Is a Typical Installation Configuration for SANPoint Control QuickStart?" on page 3

"Choosing SANPoint Control QuickStart Hosts" on page 5

Documents You Need To Plan Your Installation

You need several documents to plan your installation and work through this manual quickly and successfully. These documents are:

- *SANPoint Control QuickStart Release Notes* (`spcqs_notes.pdf`)
- *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`)

Note The *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`) is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm

- The SANPoint Control QuickStart Configuration Utility Report (see "Getting Basic Configuration Data About Your SAN" on page 49 for details on where to get this utility and how to use it)
- Diagram of your SAN (suggested for your reference)

What Is a Typical Installation Configuration for SANPoint Control QuickStart?

A typical full installation of SANPoint Control QuickStart consists of a single SANPoint Control QuickStart Server, multiple SANPoint Control QuickStart Agents, and multiple VERITAS Enterprise Administrator (VEA) Consoles. The actual number of Agent and VEA Console installations may vary according to user needs. This section provides some guidelines for deciding how to install the components on single-fabric and multi-fabric SANs.

On a single-fabric SAN, you should install the QuickStart Server on a host with a direct connection to the principal switch on the fabric. If possible, you should configure for redundant connections.

To optimize SANPoint Control QuickStart's discovery capability, you should ensure that every object on the fabric is visible to the QuickStart Server or a QuickStart Agent (that reports its discovery findings back to the QuickStart Server). You should install the Agent on as many SAN-attached hosts as possible so that SANPoint Control QuickStart can discover which hosts have OS handles for each storage device. If an object is zoned apart from all SANPoint Control QuickStart hosts on the fabric, then SANPoint Control QuickStart will not be able to fully discover that object's attributes.

You should install the VEA Console on as many client hosts as the administrator and other users require. Each client host must have network access to the QuickStart Server host; if desired, you can install the VEA Console on the same host as the SANPoint Control QuickStart Server or Agent.

Multi-Fabric SANs

On a multi-fabric SAN, you must decide whether to manage the fabrics together or individually. If the fabrics are each managed individually, then the configuration described for single-fabric SANs may be used for each fabric.

If you want to manage all fabrics from a single installation of SANPoint Control QuickStart, then you must configure your SAN as follows:

1. Install the SANPoint Control QuickStart Server on any fabric—most likely the largest or most important fabric.

2. On the same fabric as the QuickStart Server, install the SANPoint Control QuickStart Agent on as many hosts as possible.

3. On every other fabric, configure one QuickStart Agent to run the Management Explorer (MGEX). That Agent host should have a connection to the principal switch on its fabric. (You can configure an Agent to run MGEX by editing `sal.conf` on the QuickStart Server host. See "Configuring the Server for Agent Discovery" on page 66 for more information.)

4. Install other QuickStart Agent hosts on every fabric so that every object on every fabric is visible to at least one Agent host.

5. You should install the VERITAS Enterprise Administrator (VEA) Console on as many client hosts as the administrator and other users require. Each client host must have network access to the QuickStart Server host; if desired, you can install the VEA Console on the same host as the QuickStart Server or QuickStart Agent.

Caution Do not install more than one QuickStart Server on the same SAN fabric.

Choosing SANPoint Control QuickStart Hosts

In addition to the standard host requirements for SANPoint Control QuickStart, there are other factors you should consider when choosing SANPoint Control QuickStart hosts. For recommended system specifications, see the *SANPoint Control QuickStart Release Notes*.

Choosing a SANPoint Control QuickStart Server Host

In order of importance, the factors to consider when choosing a host for the SANPoint Control QuickStart Server:

- Host stability
- Connectivity with other SAN objects
- Host resources

First and foremost, choose a host that has a record of stability—long uptimes with minimal interruptions.

The QuickStart Server host should have a connection to the principal switch on your SAN fabric—redundant connections if possible. Additionally, if zones are implemented on the SAN, the QuickStart Server host should be zoned together with the switch to which it is connected.

The host's hardware resources are important primarily when using SANPoint Control QuickStart to manage a large enterprise SAN. The greater the number of objects on the SAN, the larger and more complex the QuickStart Server's object database will be, which can impact the performance of a slower host. For recommended system specifications, see the *SANPoint Control QuickStart Release Notes*.

Choosing a SANPoint Control QuickStart Agent Host

A SANPoint Control QuickStart Agent assists the SANPoint Control QuickStart Server with SAN device discovery. When objects on the SAN are zoned apart from the Server, it relies on the Agents to discover the objects and report back with information about them.

Install the Agent on as many fibre-attached hosts as possible to maximize SANPoint Control QuickStart's ability to discover all objects on the fabric. It is recommended that you install the Agent on every host on the SAN if possible, except for the host running the Server.

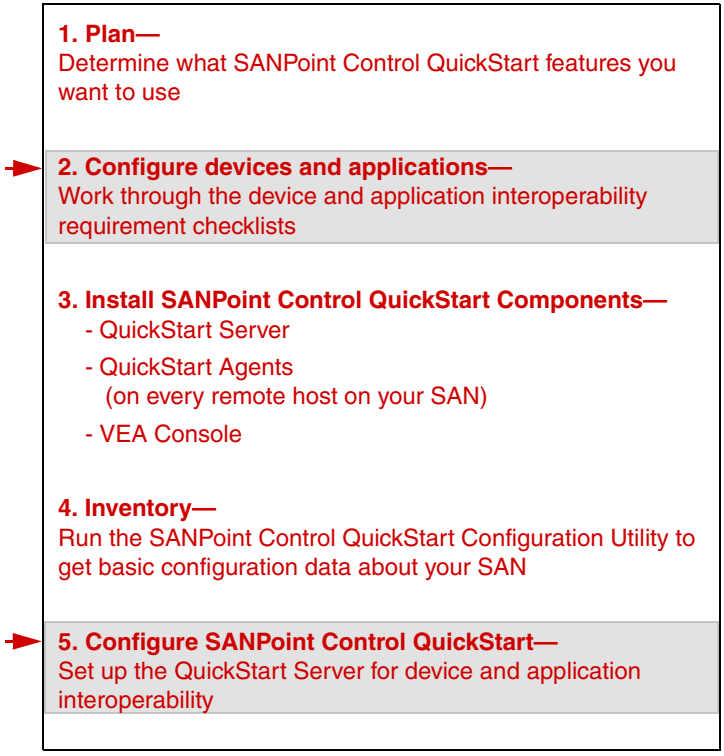
Choosing a VERITAS Enterprise Administrator (VEA) Console Host

A host running the VERITAS Enterprise Administrator (VEA) Console must have a network connection to the SANPoint Control QuickStart Server. It should also have enough memory resources to run Java-based applications like the VEA Console smoothly. For recommended system specifications, see the *SANPoint Control QuickStart Release Notes*.

Device and Application Interoperability Requirement Checklists 2

This section provides interoperability requirement checklists for SANPoint Control QuickStart to discover devices and applications.

SANPoint Control QuickStart Installation and Configuration Flowchart



You should refer to this section at two points:

1. Before installing SANPoint Control QuickStart, during device and application configuration, and

2. After installing SANPoint Control QuickStart, during SANPoint Control QuickStart Server configuration

Supported devices and applications are listed in the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*.

Note The *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`) is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm

This section contains the following topics:

"Interoperability Requirements for Applications" on page 9

"Interoperability Requirements for Switches" on page 15

"Firewall Requirements" on page 27

"Interoperability Requirements for HBAs" on page 29

"Interoperability Requirements for Bridges and Routers" on page 36

Interoperability Requirements for Applications

The sections that follow list requirements and configuration procedures for SANPoint Control QuickStart to properly discover supported applications.

"VERITAS Volume Manager Requirements" on page 10

"VERITAS NetBackup Requirements" on page 11

"VERITAS Cluster Server Requirements" on page 12

"IBM DB2 EE and EEE Requirements" on page 13

"Oracle Requirements" on page 14

VERITAS Volume Manager Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover VERITAS Volume Manager:

"Supported Versions"

"Device and Application Setup Requirements"

"SANPoint Control QuickStart Setup Requirements"

Supported Versions

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device and Application Setup Requirements

Setup. Follow application setup listed in your VERITAS Volume Manager documentation.

SANPoint Control QuickStart Setup Requirements

No additional SANPoint Control QuickStart setup is necessary for VERITAS Volume Manager.

VERITAS NetBackup Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover VERITAS NetBackup:

"Supported Versions" on page 11

"Device and Application Setup Requirements" on page 11

"SANPoint Control QuickStart Setup Requirements" on page 11

Supported Versions

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device and Application Setup Requirements

Setup. Follow application setup listed in your VERITAS NetBackup documentation.

Domain Name Service (DNS). Ensure that both the SANPoint Control QuickStart host and the NBU Master Server host names are configured to register their domain suffix with Domain Name Service (DNS).

Host access to tape drives. If two hosts have access to the same tape drive, the hosts may assign two different NetBackup names to the same drive. This setup is not correct. Assign the same name to the drive. See the NetBackup documentation.

SSO tape drives. If two hosts have access to the same tape drive, the drive may not be set up as an SSO tape drive. Set up the drive as an SSO drive. See the NetBackup documentation.

SANPoint Control QuickStart Setup Requirements

No additional SANPoint Control QuickStart setup is necessary for VERITAS NetBackup.

VERITAS Cluster Server Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover VERITAS Cluster Server:

"Supported Versions" on page 12

"Device and Application Setup Requirements" on page 12

"SANPoint Control QuickStart Setup Requirements" on page 12

Supported Versions

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device and Application Setup Requirements

Setup. Follow application setup listed in your VERITAS Cluster Server documentation.

States of cluster systems. VERITAS Cluster Server must be in the running state. Run `hasys -state` to make sure the states of the systems in the cluster are healthy. For more information, see the VERITAS Cluster Server documentation.

SANPoint Control QuickStart Setup Requirements

No additional SANPoint Control QuickStart setup is necessary for VERITAS Cluster Server.

IBM DB2 EE and EEE Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover DB2 EE and EEE:

"Supported Versions" on page 13

"Device and Application Setup Requirements" on page 13

"SANPoint Control QuickStart Setup Requirements" on page 13

Supported Versions

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device and Application Setup Requirements

Setup. Follow application setup listed in your IBM DB2 documentation.

SANPoint Control QuickStart Setup Requirements

You must run the configuration script (`vxDB2`) for the SANPoint Control QuickStart DB2 explorer to discover and monitor instances of DB2 on your SAN. The SANPoint Control QuickStart install script gives you this opportunity, or you may run the configuration script at any time on the SANPoint Control QuickStart Server. For more information, see "vxDB2" on page 98.

Oracle Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover Oracle:

"Supported Versions" on page 14

"Device and Application Setup Requirements" on page 14

"SANPoint Control QuickStart Setup Requirements" on page 14

Supported Versions

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device and Application Setup Requirements

Setup. Follow application setup listed in your Oracle documentation.

Oracle Explorer. The SANPoint Control QuickStart Oracle Explorer must be run by a user with Oracle DBA privileges

SANPoint Control QuickStart Setup Requirements

No additional SANPoint Control QuickStart setup is necessary for Oracle.

Interoperability Requirements for Switches

The sections that follow list requirements and configuration procedures for SANPoint Control QuickStart to properly discover supported switches.

"Brocade Switch Requirements" on page 16

"Cisco Switch Requirements" on page 19

"INRANGE Switch Requirements" on page 21

"McDATA Switch Requirements" on page 23

"QLogic Switch Requirements" on page 25

Brocade Switch Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover Brocade switches:

"Supported Models" on page 16

"Physical Connection Requirements" on page 16

"Device Setup Requirements" on page 16

"Firmware (Microcode) and Ancillary Software Requirements" on page 17

"SANPoint Control QuickStart Setup Requirements" on page 17

Supported Models

SilkWorm 2040, 2050, 2240, 2250, 2400, 2800, 3200, 3800, 6400, 12000

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Physical Connection Requirements

For in-band discovery, the following physical connections must be made:

- Fibre Channel connection between the SANPoint Control QuickStart Server or SANPoint Control QuickStart Agent host where the Management explorer (MGEX) is doing in-band discovery and the fabric where the Brocade switch is located.

Device Setup Requirements

Switch names. Switches in the SAN must have unique names.

QuickLoop issues. QuickLoop mode is the default mode; however, it can sometimes prevent HBAs from connecting to the SAN fabric. If you experience that problem, disable QuickLoop mode. For more information, refer to your Brocade documentation.

QuickLoop visualization. Because Brocade switch ports can be configured independently, some ports may be set to Fabric mode and others to QuickLoop mode. Switch ports in QuickLoop mode will display correctly in SANPoint Control QuickStart and can be zoned, but you won't see fibre-attached objects in the Topology Map.

Out-of-band discovery and in-context launching of third party applications. When doing out-of-band discovery or to enable in-context launching of third-party applications, configure the switch for out-of-band addressing (IP address, host name, or fully qualified domain name of the SANPoint Control QuickStart Server). For more information, refer to your Brocade documentation.

Subnets. To utilize SANPoint Control QuickStart out-of-band discovery and reports, the switch must not be isolated on a separate subnet. The switch should be accessible through IP by the host on which the SANPoint Control QuickStart Server will be installed. If the switch is on a different subnet, add the appropriate routing table entry on the host. If no router exists, you may need to configure the host as a router with a network interface to each subnet.

Zone aliases. SANPoint Control QuickStart supports zone alias visualization for Brocade fabrics. For more information, refer to your Brocade documentation.

Firmware (Microcode) and Ancillary Software Requirements

For required firmware (microcode) and ancillary software, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go toVERITAS Support the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

SANPoint Control QuickStart Setup Requirements

No additional SANPoint Control QuickStart setup is necessary for Brocade switches if you have a direct Fibre Channel connection from the SANPoint Control QuickStart Server to the switch. (SANPoint Control QuickStart discovers the switch using the Management explorer [MGEX] in-band.)

You must configure the SANPoint Control QuickStart Server if your Brocade switches use non-default login credentials (a username that is not `admin` and a password that is not `password`). For more information, see "Adding or Modifying Brocade Switch Credentials" on page 72.

If there is a SANPoint Control QuickStart Agent host with a Fibre Channel connection to the Brocade switch, then you can discover the switch using the HBA and MGEX explorers that run on the Agent. You must configure the SANPoint Control QuickStart Server with the SANPoint Control QuickStart Agent host name, IP address, or qualified domain name and with MGEX discovery enabled on the Agent (**Enable switch exploration** checkbox selected). For more information, see "Configuring the Server for Agent Discovery" on page 66.

To perform MGEX out-of-band exploration, you must configure the SANPoint Control QuickStart Server with each Brocade switch name, IP address, or fully qualified domain name for the switch in the SANPoint Control QuickStart Server SAN discovery configuration file (`/var/VRTSspcq/sal.conf`). Using a text editor, update `SwitchNameList` under `[MGEX]` and restart the SANPoint Control QuickStart Server. For more information, see "Stopping and Starting SANPoint Control QuickStart" on page 84.

Cisco Switch Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover switches:

"Supported Models" on page 19

"Physical Connection Requirements" on page 19

"Device Setup Requirements" on page 19

"Firmware (Microcode) and Ancillary Software Requirements" on page 20

"SANPoint Control QuickStart Setup Requirements" on page 20

Supported Models

MDS 9509, 9216

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Physical Connection Requirements

For full discovery, make a network connection between the SANPoint Control QuickStart Server and each Cisco switch.

Device Setup Requirements

Switch names. Switches in the SAN must have unique names.

Out-of-band discovery and in-context launching of third party applications. When doing out-of-band discovery or to enable in-context launching of third-party applications, configure the switch for out-of-band addressing (IP address, host name, or fully qualified domain name of the SANPoint Control QuickStart Server). For more information, refer to your Cisco documentation.

Subnets. To utilize SANPoint Control QuickStart out-of-band discovery and reports, the switch must not be isolated on a separate subnet. The switch should be accessible through IP by the host on which the SANPoint Control QuickStart Server is installed. If the switch is on a different subnet, add the appropriate routing table entry on the host. If no router exists, you may need to configure the host as a router with a network interface to each subnet.

SNMP Credentials. The following SNMP version-specific requirements (consistent with the requirements for the Cisco Fabric Manager) apply:

- SNMP v1 or v2c—
  All Cisco switches using either SNMP version 1 or version 2c must share the same SNMP read/write community name.

Note `spcconfig` does not discover Cisco MDS switches that use SNMP v2x or v3.

- SNMP v3—
  SANPoint Control QuickStart requires that the SNMP v3 credentials for the switch be network-admin or some other role with read/write permissions. This network-admin account must be set up across all Cisco switches. The SANPoint Control QuickStart Server stores SNMP v3 credentials in its credential database.

Tip You can create multiple sets of credentials on the same Cisco MDS switch. To verify switch SNMP information, from the MDS switch, run this Cisco CLI command: **`show snmp`**

Firmware (Microcode) and Ancillary Software Requirements

For required firmware (microcode) and ancillary software, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document:
http://seer.support.veritas.com/docs/260958.htm.

SANPoint Control QuickStart Setup Requirements

You must configure the SANPoint Control QuickStart Server by editing the SAN discovery configuration file (`sal.conf`) and then restarting `vxsal`. For more information, see "Configuring the Server for Cisco MDS Switch Discovery" on page 68.

INRANGE Switch Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover INRANGE switches:

"Supported Models" on page 21

"Physical Connection Requirements" on page 21

"Device Setup Requirements" on page 22

"Firmware (Microcode) and Ancillary Software Requirements" on page 22

"SANPoint Control QuickStart Setup Requirements" on page 22

Supported Models

FC/9000–8, FC/9000–16, FC/9000–64, FC/9000–128

The FC/9000-8 and FC/9000-16 are discovered and managed out-of-band via the SANPoint Control SNMP explorer.

The FC 16-2 is discovered out-of-band via the SANPoint Control SNMP explorer and is managed in-band via the SANPoint Control Management explorer [MGEX].

The FC/9000–64 and FC/9000–128 can be discovered in-band or out-of-band, or both, depending on the firmware version in the switch. See the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* to determine how these switches are discovered.

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Physical Connection Requirements

For switches discovered in-band, make the following physical connection:

- Fibre Channel connection between the SANPoint Control QuickStart Server or SANPoint Control QuickStart Agent host where the Management explorer (MGEX) is doing in-band discovery and the fabric where the INRANGE switch is located.

For switches discovered out-of-band, make the following physical connection:

- Network connection between the SANPoint Control QuickStart Server and each switch

Device Setup Requirements

No additional device setup is necessary for INRANGE switches.

Firmware (Microcode) and Ancillary Software Requirements

For required firmware (microcode) and ancillary software, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

SANPoint Control QuickStart Setup Requirements

For switches discovered via a Management explorer running on a SANPoint Control QuickStart Server host with a Fibre Channel connection to the INRANGE switches, no further SANPoint Control QuickStart setup is required.

For switches discovered or managed via a Management explorer running on a SANPoint Control QuickStart Agent host with a Fibre Channel connection to the INRANGE switches, configure the SANPoint Control QuickStart Server with the SANPoint Control QuickStart Agent host name, IP address, or qualified domain name and with MGEX discovery enabled on the Agent (**Enable switch exploration** checkbox selected). For more information, see "Configuring the Server for Agent Discovery" on page 66.

For switches discovered via the SANPoint Control QuickStart SNMP explorer, you must configure the SANPoint Control QuickStart Server with each INRANGE switch name, IP address, or fully qualified domain name for the switch in the SANPoint Control QuickStart Server SAN discovery configuration file (`/var/VRTSspcq/sal.conf`). Using a text editor, update `SwitchNameList` under `[Exp.SNMP]` and restart the SANPoint Control QuickStart Server. For more information, see "Stopping and Starting SANPoint Control QuickStart" on page 84.

McDATA Switch Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover McDATA switches:

"Supported Models" on page 23

"Physical Connection Requirements" on page 23

"Device Setup Requirements" on page 23

"Firmware (Microcode) and Ancillary Software Requirements" on page 24

"SANPoint Control QuickStart Setup Requirements" on page 24

Supported Models

ED–5000, ED–6064, ES–1000, ES–3016, ES–3032, ES–3216, ES–3232

All switches, except the ES–1000, can be discovered in-band, via the SANPoint Control Management explorer [MGEX], or out-of-band, via the SANPoint Control SNMP explorer. The ES–1000 is discovered out-of-band.

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Physical Connection Requirements

For switches discovered in-band, make the following physical connections:

- Fibre Channel connection between the SANPoint Control QuickStart Server or SANPoint Control QuickStart Agent where the Management explorer (MGEX) is doing in-band discovery and the fabric where the McDATA switch is located.

For switches discovered out-of-band, make the following physical connection:

- Network connection between the SANPoint Control QuickStart Server and each switch

Device Setup Requirements

No additional device setup is necessary for McDATA switches.

Firmware (Microcode) and Ancillary Software Requirements

For required firmware (microcode) and ancillary software, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document:
http://seer.support.veritas.com/docs/260958.htm.

SANPoint Control QuickStart Setup Requirements

For switches discovered or managed via a Management explorer running on a SANPoint Control QuickStart Server host with a Fibre Channel connection to the McDATA switches, no further setup is required.

For switches that are discovered or managed via a Management explorer running on a SANPoint Control QuickStart Agent host with a Fibre Channel connection to the McDATA switches, configure the SANPoint Control QuickStart Server with the SANPoint Control QuickStart Agent host name, IP address, or qualified domain name and with MGEX discovery enabled on the Agent (**Enable switch exploration** checkbox selected). For more information, see "Configuring the Server for Agent Discovery" on page 66.

QLogic Switch Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover QLogic switches:

"Supported Models" on page 25

"Physical Connection Requirements" on page 25

"Device Setup Requirements" on page 25

"Firmware (Microcode) and Ancillary Software Requirements" on page 25

"SANPoint Control QuickStart Setup Requirements" on page 26

Supported Models

SANBox–8, SANBox–16, SANBox2–16

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Physical Connection Requirements

There must be a network connection between the SANPoint Control QuickStart Server and each switch.

Device Setup Requirements

No additional device setup is necessary for QLogic switches.

Firmware (Microcode) and Ancillary Software Requirements

For required firmware (microcode) and ancillary software, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

SANPoint Control QuickStart Setup Requirements

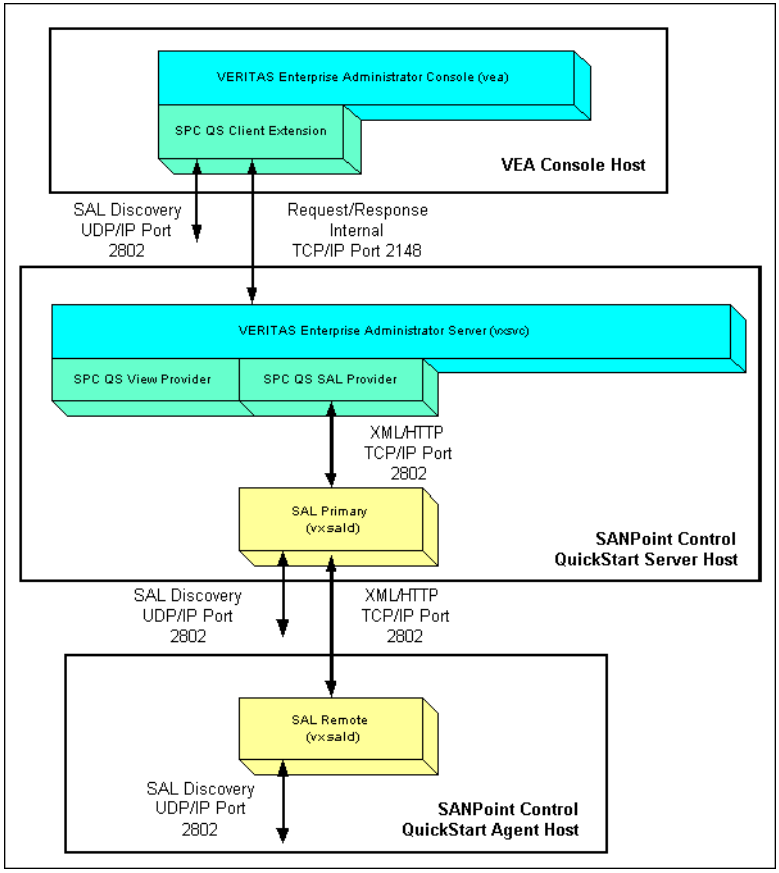
For switches discovered via the SANPoint Control QuickStart SNMP explorer, you must configure the SANPoint Control QuickStart Server with each QLogic switch name, IP address, or fully qualified domain name for the switch in the SANPoint Control QuickStart Server SAN discovery configuration file (`/var/VRTSspcq/sal.conf`). Using a text editor, update `SwitchNameList` under `[Exp.SNMP]` and restart the SANPoint Control QuickStart Server. For more information, see "Stopping and Starting SANPoint Control QuickStart" on page 84.

Firewall Requirements

For the SANPoint Control QuickStart Server, Agent, and VEA Console to communicate across a firewall the following requirements must be met:

- The firewall must be configured to allow `http` access to several specific ports
- A range of ports for sending information must be specified in the SANPoint Control QuickStart Server

SANPoint Control QuickStart Communication Ports



The following table lists the default ports that SANPoint Control QuickStart environment uses for information transfer:

Default Ports Utilized In a SANPoint Control QuickStart Installation

Port	Protocol	Initiator > Recipient Purpose	Impact if Blocked
2148	TCP/IP	VEA Console > VEA Server VEA Server > VEA Console VEA client - server communication	Console cannot communicate with the QuickStart Server
2802	TCP/IP	VEA Server > QuickStart Server QuickStart Server > VEA Server QuickStart Server > QuickStart Agent QuickStart Agent > QuickStart Server VEA server – SAL primary communication	No SAN objects in Console
2802	UDP	Console > Agent Agent > Console Agent discovery	Console cannot locate Agents

In addition, to ensure the proper number of ports are available, you must establish a port range for the QuickStart Server to send information to the VEA Console across the firewall. Use a text editor to edit the `PortRange` entry in the SAN discovery configuration file (`/opt/VRTSsal/sal.conf`) and then restart vxsal. For more information, see "vxsal" on page 131.

All the default SANPoint Control QuickStart ports are registered with IANA (Internet Assigned Numbers Authority); however, you can change most of them when necessary.

Interoperability Requirements for HBAs

The sections that follow list requirements and configuration procedures for SANPoint Control QuickStart to properly interoperate with supported vendor host bus adapters (HBAs).

"Emulex HBA Requirements" on page 30

"JNI HBA Requirements" on page 32

"QLogic HBA Requirements" on page 34

Emulex HBA Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover Emulex HBAs:

"Supported Versions" on page 30

"Firmware Requirements" on page 30

"Device Setup Requirements" on page 30

"SANPoint Control QuickStart Setup Requirements" on page 31

Supported Versions

LP8000, LP8000S, LP9000, LP9002S, LP9802DC

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Firmware Requirements

For required firmware (microcode) and ancillary software, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device Setup Requirements

Installation sequence. On UNIX systems, after downloading and using `pkadd` to install the driver, you must make sure that the HBA is configured for point-to-point mode. Using a text editor, open the Emulex configuration file (`/kernel/drv/lpfc.conf`) set topology to `2`, and then reboot the host.

For example:

```
#topology:link topology for initializing the Fibre Channel connection.
# 0 = attempt loop mode, if it fails attempt point-to-point mode
# 2 = attempt point-to-point mode only
# 4 = attempt loop mode only
```

```
# 6 = attempt point-to-point mode, if it fails attempt loop mode
# Set point-to-point mode if you want to run as an N_Port.
# Set loop mode if you want to run as an NL_Port.
topology=2;
```

CT passthru support. The firmware must be flash-updated to the version required by SANPoint Control QuickStart. The firmware that is supplied from the factory does not work with the HBA driver that is needed to support CT passthru. If the HBA has the correct HBA driver but the incorrect firmware, you may receive inconsistent information from the HBA driver. To flash-update the HBA, see your vendor documentation.

Loop Mode. Many HBAs have Loop Mode enabled by default. You must enable point-to-point or Fabric mode for your HBAs to work correctly with SANPoint Control QuickStart. If you don't, SANPoint Control QuickStart won't discover the fabric. To configure the HBA, see your vendor documentation.

Port driver topology. Change the port driver topology to Point-to-Point mode. To configure the HBA, see your vendor documentation.

World Wide Names (WWNs). The default Emulex driver settings cause all Emulex HBAs installed in the same host to use the same node WWN. This will cause SANPoint Control QuickStart to discover a single node WWN and create a single HBA object with the total number of ports for all the physical HBAs in the host. To have each HBA use its own unique node WWN, configure each HBA, then reboot the host. See your vendor documentation for details.

Host reboot. Also, after disconnecting an HBA from a fabric switch, and then reconnecting it, you may have to reboot the host. Some HBAs cannot log in to a fabric again after they have logged out.

SANPoint Control QuickStart Setup Requirements

No additional SANPoint Control QuickStart setup is necessary for Emulex HBAs

JNI HBA Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover JNI HBAs:

"Supported Versions" on page 32

"Firmware Requirements" on page 32

"Device Setup Requirements" on page 32

"SANPoint Control QuickStart Setup Requirements" on page 33

Supported Versions

FCI–1063, FC64–1063, FCE–1063, FCE2–1063, FCE–6410, FCE2–6412, FCE–6460, FCE–1473

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Firmware Requirements

For required firmware (microcode) and ancillary software, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device Setup Requirements

Setup. Follow setup listed in your JNI documentation.

JNI HBA configuration file. To configure the JNI card to work with SANPoint Control QuickStart, you should change from default loop mode to fabric mode and reboot. Using `pkgadd`, install the JNI driver on the host. Using a text editor, open the configuration file for JNI (`/kernel/drv/fca-pci.conf`) and set `fca_nport` to `1`. For example:

```
# Configuration flag fca_nport
# Type: boolean; default: 0 (false)
# If false (0), then fca initializes on a loop
# If true (1), then fca initializes as an N_Port
```

```
#    and fabric operation is enabled
fca_nport = 1;
```

Host reboot. After disconnecting an HBA from a fabric switch, and then reconnecting it, you may have to reboot the host. Some HBAs cannot log in to a fabric again after they have logged out.

FCE–64xx HBAs for Solaris. Use the JNI utility EZ Fibre version 2.2 or later to configure FCE–64xx HBAs for Solaris. For more information, refer to your JNI documentation.

SANPoint Control QuickStart Setup Requirements

No additional SANPoint Control QuickStart setup is necessary for JNI HBAs.

QLogic HBA Requirements

The following sections list requirements for SANPoint Control QuickStart to properly discover QLogic HBAs:

"Supported Versions" on page 34

"Firmware Requirements" on page 34

"Device Setup Requirements" on page 34

"SANPoint Control QuickStart Setup Requirements" on page 35

Supported Versions

QLA 2200F, QLA 2202F, QLA 2202FS, QLA 2300, QLA 2310, QLA 2340, QLA 2342

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Firmware Requirements

For required firmware (microcode) and ancillary software, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device Setup Requirements

Setup. Follow setup listed in your QLogic documentation.

Fabric mode. By default, QLogic HBA ports are configured in Fabric mode. If your QLogic card is not configured in Fabric mode, you must do so manually by editing the driver configuration. See your vendor documentation for details.

Host reboot. After disconnecting an HBA from a fabric switch, and then reconnecting it, you may have to reboot the host. Some HBAs cannot log in to a fabric again after they have logged out.

SANPoint Control QuickStart Setup Requirements

No additional SANPoint Control QuickStart setup is necessary for QLogic HBAs.

Interoperability Requirements for Bridges and Routers

The sections that follow list requirements and configuration procedures for SANPoint Control QuickStart to properly interoperate with supported vendor bridges and routers.

"Cisco Router Requirements" on page 37

"Chaparral Bridge Requirements" on page 38

"Crossroads Bridge Requirements" on page 39

"Hewlett-Packard Bridge Requirements" on page 40

Cisco Router Requirements

The following sections list requirements for SANPoint Control QuickStart to properly interoperate with Cisco iSCSI routers.

"Supported Versions" on page 37

"Device Setup Requirements" on page 37

"SANPoint Control QuickStart Setup Requirements" on page 37

Supported Versions

Cisco 5420 F/W 1.3 and 1.5

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device Setup Requirements

Setup. Follow setup listed in your Cisco documentation.

Hosts with iSCSI HBAs. If a host is attached to the SAN via an iSCSI HBA connected to an iSCSI router, it might not be automatically registered for DNS. In that case, SANPoint Control QuickStart will not be able to resolve the hostname from the HBA address and will not discover the host. You must ensure that iSCSI HBAs are added to the appropriate database for system resolver functions to resolve the hostname from the iSCSI HBA address.

SANPoint Control QuickStart Setup Requirements

Configure the SANPoint Control QuickStart Server for each Cisco router to be discovered. For more information, see "Configuring the Server for Bridge and Router Discovery" on page 74.

Chaparral Bridge Requirements

The following sections list requirements for SANPoint Control QuickStart to properly interoperate with Chaparral bridges:

"Supported Versions" on page 38

"Device Setup Requirements" on page 38

"SANPoint Control QuickStart Setup Requirements" on page 38

Supported Versions

Chaparral 2620 F/W S500/S500R01c

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device Setup Requirements

Setup. Follow setup listed in your Chaparral documentation.

SANPoint Control QuickStart Setup Requirements

Configure the SANPoint Control QuickStart Server for each Chaparral bridge to be discovered. For more information, see "Configuring the Server for Bridge and Router Discovery" on page 74.

Crossroads Bridge Requirements

The following sections list requirements for SANPoint Control QuickStart to properly interoperate with Crossroads bridges:

"Supported Versions" on page 39

"Device Setup Requirements" on page 39

"SANPoint Control QuickStart Setup Requirements" on page 39

Supported Versions

4150 F/W 3.02 2006x, 4250 F/W 3.02 2005c, 4450 F/W 3.02 2006x, 4200 F/W 2.2 9912e

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device Setup Requirements

Setup. Follow setup listed in your Crossroads documentation.

SANPoint Control QuickStart Setup Requirements

Configure the SANPoint Control QuickStart Server for each Crossroads bridge to be discovered. For more information, see "Configuring the Server for Bridge and Router Discovery" on page 74.

Hewlett-Packard Bridge Requirements

The following sections list requirements for SANPoint Control QuickStart to properly interoperate with Hewlett-Packard bridges:

"Supported Versions" on page 40

"Device Setup Requirements" on page 40

"SANPoint Control QuickStart Setup Requirements" on page 40

Supported Versions

Surestore 2/1 LV (4250) F/W 3.02 2006j

For the latest support information, see the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (`spcqs_suptmx.pdf`), which is included in the SANPoint Control QuickStart documentation package `/opt/VRTSspqdc`. Because SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm.

Device Setup Requirements

Setup. Follow setup listed in your Hewlett-Packard documentation.

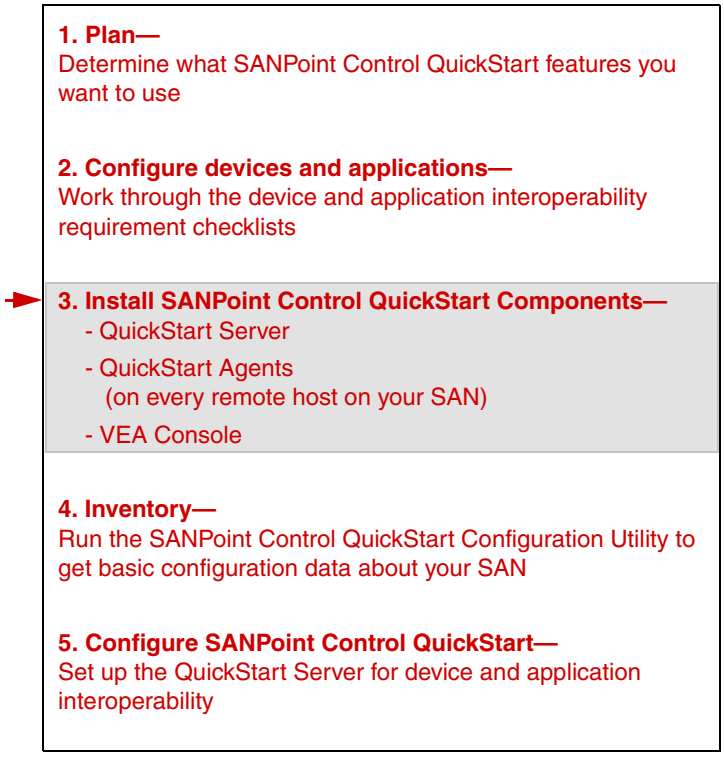
SANPoint Control QuickStart Setup Requirements

Configure the SANPoint Control QuickStart Server for each Hewlett-Packard bridge to be discovered. For more information, see "Configuring the Server for Bridge and Router Discovery" on page 74.

Installing SANPoint Control QuickStart 3

This section describes how to install SANPoint Control QuickStart.

SANPoint Control QuickStart Installation and Configuration Flowchart



This section contains the following topics:

"Installing the SANPoint Control QuickStart Server" on page 42

"Installing the SANPoint Control QuickStart Agent" on page 44

"Installing the VERITAS Enterprise Administrator (VEA) Console" on page 46

Installing the SANPoint Control QuickStart Server

This section describes how to use the SANPoint Control QuickStart install script to install the SANPoint Control QuickStart Server on a Solaris host system.

Caution Do not install more than one QuickStart Server on a given fabric. Doing so might cause SAN discovery data to be corrupted.

Note For information about installing language-related packages, consult the *Storage Solutions Installation Guide*.

▼ To install the SANPoint Control QuickStart Server

1. Locate your VERITAS Storage Solutions software license key.

   To obtain a license key, contact your VERITAS Sales Representative.

2. Log on to the target host as root.

3. On the target host, mount VERITAS Storage Solutions software disc 2.

4. Change to the `sanpoint_control_quickstart` directory.

5. Type the following command and press Enter or Return:

   `./installspcq`

   The SANPoint Control QuickStart install script displays a welcome message.

   ```
   Welcome to the VERITAS SANPoint Control QuickStart
   installation for Unix platforms.

   Press [Return] to continue:
   ```

6. Press Enter or Return.

   The SANPoint Control QuickStart install script displays a prompt asking if you want to install the QuickStart Server or QuickStart Agent.

   ```
   1)  Install Server
   2)  Install Agent

   Please enter '1' to install the Server, '2' to install an Agent:
   [1-2,q] (2)
   ```

7. Type **`1`** and press Enter or Return to begin the installation.

During installation, the SANPoint Control QuickStart install script presents prompts for:

- System names—
  Supply the name, IP address, or fully qualified domain name of the host on which you want to install the QuickStart Server.
- Optional packages—
  You can optionally install the VERITAS Enterprise Administrator (VEA) Console and the SANPoint Control QuickStart documentation and manual pages. If you want to install the VERITAS Enterprise Administrator (VEA) Console *only*, see the section, "Installing the VERITAS Enterprise Administrator (VEA) Console" on page 46.
- VERITAS Storage Solutions software license key—
  Type your VERITAS Storage Solutions software license key and press Enter or Return.
- Oracle explorer configuration—
  Under normal circumstances, you do not need to configure the Oracle explorer manually; it will be auto-configured. You must configure the explorer only if SANPoint Control QuickStart is not discovering Oracle instances on the QuickStart Server host. For more information, see "vxOra" on page 100.
- SAN device configuration data—
  The SANPoint Control QuickStart Configuration Utility (`spcconfig`) scans your SAN for supported hardware and software and identifies configuration problems in a report that it outputs. This inventory report—in both HTML and comma-separated value (CSV) files—lists supported devices, whether they meet SANPoint Control QuickStart requirements, and, if necessary, what to do to change their configuration. For more information, see "Getting Basic Configuration Data About Your SAN" on page 49.

When installation is complete, the SANPoint Control QuickStart install script displays a message similar to the following:

```
Installation of SANPoint Control QuickStart 4.0 has completed
successfully.
```

After you install the QuickStart Server, you must install a SANPoint Control QuickStart Agent on every host in your SAN. For more information, see "Installing the SANPoint Control QuickStart Agent" on page 44.

Installing the SANPoint Control QuickStart Agent

For the most complete and accurate SAN discovery, install the SANPoint Control QuickStart Agent on every host in your SAN. The QuickStart Agent consists of several SAN explorers that are also used by the SANPoint Control QuickStart Server, including the Cisco MDS explorer, Management Server explorer (MGEX), the SNMP explorer, and the HBA explorer, based on SAN Access Layer technology.

Client applications such as the VERITAS Enterprise Administrator (VEA) Console cannot connect to a SANPoint Control QuickStart Agent host, and the QuickStart Agent cannot run on the same host as the QuickStart Server.

This section describes how to run the SANPoint Control QuickStart install script to install the Agent and its dependencies on a Solaris host.

Note For information about installing language-related packages, consult the *Storage Solutions Installation Guide*.

▼ To install the SANPoint Control QuickStart Agent

1. Locate your VERITAS Storage Solutions software license key.

   To obtain a license key, contact your VERITAS Sales Representative.

2. Log on to the target host as root.

3. On the target host, mount VERITAS Storage Solutions software disc 2.

4. Change to the `sanpoint_control_quickstart` directory.

5. Type the following command and press **Enter** or **Return**:

   `./installspcq`

   The SANPoint Control QuickStart install script displays a welcome message.

   ```
   Welcome to the VERITAS SANPoint Control QuickStart
   installation for Unix platforms.

   Press [Return] to continue:
   ```

6. Press Enter or Return.

   The SANPoint Control QuickStart install script displays a prompt asking if you want to install the QuickStart Server or QuickStart Agent.

   ```
   1)  Install Server
   ```

```
2)  Install Agent

Please enter '1' to install the Server, '2' to install an Agent:
[1-2,q] (2)
```

7. Type **2** and press Enter or Return to begin the installation.

   During installation, the SANPoint Control QuickStart install script presents prompts for:

   - System names—
     Supply the name, IP address, or fully qualified domain names of the hosts on which you want to install the QuickStart Agent.
   - Optional packages—
     You can optionally install the VERITAS Enterprise Administrator (VEA) Console and the SANPoint Control QuickStart documentation and manual pages. If you want to install the VERITAS Enterprise Administrator (VEA) Console *only*, see the section, "Installing the VERITAS Enterprise Administrator (VEA) Console" on page 46.
   - VERITAS Storage Solutions software license key—
     Type your VERITAS Storage Solutions software license key and press Enter or Return.
   - Oracle explorer configuration—
     Under normal circumstances you do not need to configure the Oracle explorer manually; they will be auto-configured. You must configure the explorers only if SANPoint Control QuickStart is not discovering Oracle instances on the QuickStart Server host. For more information, see "vxOra" on page 100.
   - SAN device configuration data—
     The SANPoint Control QuickStart Configuration Utility (`spcconfig`) scans your SAN for supported hardware and software and identifies configuration problems in a report that it outputs. This inventory report—in both HTML and comma-separated value (CSV) files—lists supported devices, whether they meet SANPoint Control QuickStart requirements, and, if necessary, what to do to change their configuration. For more information, see "Getting Basic Configuration Data About Your SAN" on page 49.

   When installation is complete, the SANPoint Control QuickStart install script displays a message similar to the following:

   ```
   Installation of SANPoint Control QuickStart 4.0 has completed
   successfully.
   ```

After you install the QuickStart Agent, you need to install one or more VERITAS Enterprise Administrator (VEA) Consoles. See the section, "Installing the VERITAS Enterprise Administrator (VEA) Console" on page 46.

Installing the VERITAS Enterprise Administrator (VEA) Console

The VERITAS Enterprise Administrator (VEA) Console displays the XML data received from the SANPoint Control QuickStart Server in graphical form and provides a user interface for the many tools and functions in SANPoint Control QuickStart.

The VEA Console is an optional package that you can choose when you install the QuickStart Server and the QuickStart Agent; however, this section describes how you can install the VEA Console *singularly* on either Solaris or Windows 2000.

Note For information about installing language-related packages, consult the *Storage Solutions Installation Guide*.

▼ To install the VEA Console on Solaris

1. Log on to the Solaris host as root.
2. On the target host, mount VERITAS Storage Solutions software disc 1.

   For more information about mounting a software disc, refer to the *Storage Solutions Installation Guide* located at the root of the software disc (`storage_solutions_ig.pdf`).
3. Change directory to a location on your host where you can copy the VEA Console install package.
4. Copy the VEA Console package from the software disc to the target host (to the directory you specified in step 3), by typing the following command and pressing Enter or Return:

   `cp /cdrom/cdrom0/storage_foundation/pkgs/VRTSobgui.tar.gz .`
5. Uncompress the compressed packages, by typing the following command and pressing Enter or Return:

   `/cdrom/cdrom0/storage_foundation/scripts/install/gunzip VRTSobgui.tar.gz`
6. Extract the archived files by typing the following command and pressing Enter or Return:

   `tar xv VRTSobgui.tar`
7. Install the VEA Console (`VRTSobgui`), by typing the following command and pressing Enter or Return:

```
pkgadd -d ./pkgs VRTSobgui
```

8. Follow the `pkgadd` prompts.

For more information, consult your Solaris manual pages for `pkgadd`.

After you install the VEA Console, you need to configure the SANPoint Control QuickStart Server for device and application interoperability. See "Device and Application Interoperability Requirement Checklists" on page 7.

▼ To install the VEA Console on Windows

1. Log on to the Windows host as a user with Administrator privileges.
2. Mount VERITAS Storage Solutions software disc 1.
3. From the **Start** menu, choose **Run**.
4. Type the following in the **Open** field and press the Return key:

   ***D*:\win32\VRTSobgui.msi**

   where ***D*** is the letter of your CD-ROM drive.

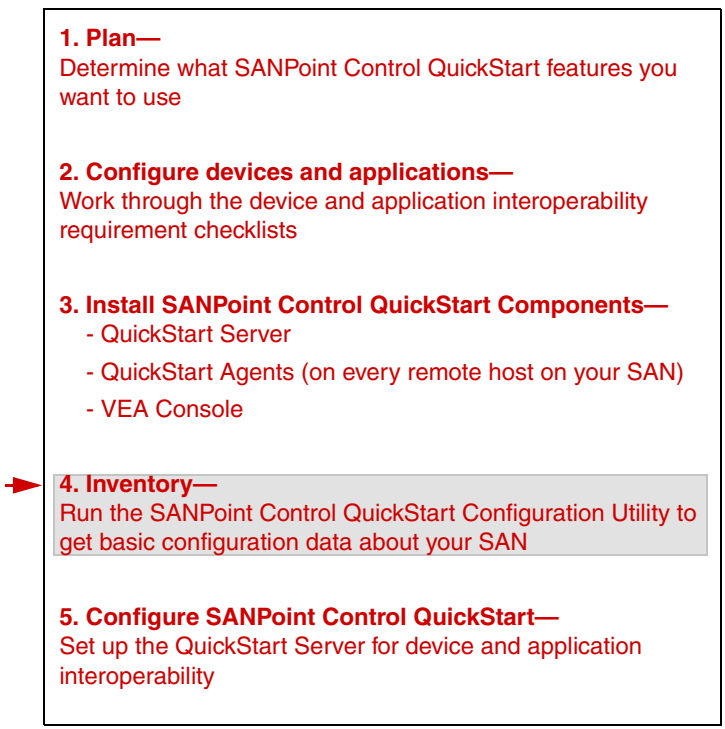
   The **Welcome** panel of the Microsoft Windows Installer Wizard displays.
5. Select **Next** and follow the remaining Installer Wizard panels.

After you install the VEA Console, you need to configure the SANPoint Control QuickStart Server for device and application interoperability. See "Device and Application Interoperability Requirement Checklists" on page 7.

Getting Basic Configuration Data About Your SAN 4

This section provides information about the SANPoint Control QuickStart Configuration Utility (`spcconfig`), including steps you take to run the utility and inventory your SAN. In a typical SANPoint Control QuickStart installation, this section corresponds to step 4 in the SANPoint Control QuickStart Installation and Configuration Flowchart below.

SANPoint Control QuickStart Installation and Configuration Flowchart



This section contains the following topics:

"Understanding the SANPoint Control QuickStart Configuration Utility" on page 51

"Running the SANPoint Control QuickStart Configuration Utility" on page 53

"Viewing the SANPoint Control QuickStart Configuration Utility Report" on page 57

"Manually Updating the Compatibility List" on page 59

Understanding the SANPoint Control QuickStart Configuration Utility

The SANPoint Control QuickStart Configuration Utility (`spcconfig`) is a utility that scans your SAN for hardware and software and identifies configuration problems in an inventory report output to both HTML and comma-separated value (CSV) formats. The report lists supported devices, whether they meet SANPoint Control QuickStart requirements, and, if necessary, what to do to change their configuration.

When you run `spcconfig`, it performs the following:

- HBA compatibility scan—sweeps the local host (a SANPoint Control QuickStart Server or Agent) for HBA drivers to compare them against the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*.

Depending upon the options you specify, `spcconfig` can perform the following on a SANPoint Control QuickStart Server host:

- SAN device compatibility scan—performs an SNMP (Simple Network Management Protocol) sweep of one or subnets to determine if your SAN devices have compatible firmware. Device scans can only be specified when running `spcconfig` from a SANPoint Control QuickStart Server host, and can take several minutes on large networks.

  Note `spcconfig` does not discover Cisco MDS switches that use SNMP v2x or v3.

- Enabling out-of-band communication—when run on a SANPoint Control QuickStart Server host, `spcconfig` can update the QuickStart Server's SAN discovery configuration file (`sal.conf`) with device IP addresses discovered during a device scan to enable out-of-band communication mechanisms. Depending upon the type of SAN devices discovered, `spcconfig` updates the `sal.conf` out-of-band-related sections such as: `[MGEX]`, `[Exp.SNMP]`, `[Exp.Array]`, `[Exp.Bridge]`, and `[Exp.CiscoMDS]`. `spcconfig` backs up the configuration file prior to making modifications. In order for the `sal.conf` changes to take effect, `spcconfig` also restarts the SAN Access Layer (SAL) process on the host.

One Section of the SANPoint Control QuickStart Configuration Utility HTML Report

Host Information

Host Name	tenterhooks
IP Addresses	255.255.255.255
OS	SunOS 5.8 **Patches required for Storage Manager Console** - 112003-02 108652-37 108940-40 108921-13 108773-12 108528-14 111293-04 108827-17. Action: Install these patches.

You can use the `spcconfig` inventory report, the device interoperability requirement checklists in "Device and Application Interoperability Requirement Checklists" on page 7, and the most current version of the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* to take advantage of the SANPoint Control QuickStart features you need. You can access the latest version of the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* at the following URL: http://seer.support.veritas.com/docs/260958.htm.

Running the SANPoint Control QuickStart Configuration Utility

In addition to running `spcconfig` on the SANPoint Control QuickStart Server host, you should run `spcconfig` on every host on your SAN on which you have installed or plan to install a SANPoint Control QuickStart Agent. If you update any devices or remove any unsupported HBAs, re-run `spcconfig`.

▼ To run the SANPoint Control QuickStart Configuration Utility

1. From the local host on which you want to run `spcconfig`, open a UNIX console and log in as `root` (UNIX).

2. Change to the `spcconfig` install directory. By default:

   ```
   /opt/VRTSspcfg/SunOS
   ```

   Tip SANPoint Control QuickStart creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to access the SANPoint Control QuickStart scripts and commands.

3. Decide which of the following `spcconfig` commands you want to use:

   SANPoint Control QuickStart Configuration Utility Command Summary

How Do You Want to Run spcconfig?	Use This Command...
Interactive mode	`spcconfig`
Interactive mode: • HBA compatibility scan and array software scan only	`spcconfig -r`
Interactive mode: • Update QuickStart Server config file for out-of-band communication?—yes	`spcconfig -u`

SANPoint Control QuickStart Configuration Utility Command Summary

How Do You Want to Run spcconfig?	Use This Command...
Non-interactive (silent) mode: • Update QuickStart Server config file for out-of-band communication?—no • Report output directory—`spcconfig` installation directory • Use the matrix on the Web?—no • Would you like to scan the network?—yes • Would you like to scan different subnets?—no	`spcconfig -d`
Non-interactive (silent) mode: • Update QuickStart Server config file for out-of-band communication?—no • Report output directory—user-defined directory • Use the matrix on the Web?—no • Would you like to scan the network?—yes • Would you like to scan different subnets?—no	`spcconfig -d --report-dir /mydir`
Non-interactive (silent) mode: • Update QuickStart Server config file for out-of-band communication?—yes • Report output directory—`spcconfig` installation directory • Use the matrix on the Web?—no • Would you like to scan the network?—yes • Would you like to scan different subnets?—no	`spcconfig -d -u`

SANPoint Control QuickStart Configuration Utility Command Summary

How Do You Want to Run spcconfig?	Use This Command...
Non-interactive (silent) mode: • Update QuickStart Server config file for out-of-band communication?—yes • Report output directory—user-defined directory • Use the matrix on the Web?—no • Would you like to scan the network?—yes • Would you like to scan different subnets?—no	`spcconfig -d -u --report-dir /mydir`
Non-interactive (silent) mode: • HBA compatibility scan and array software scan only	`spcconfig -r -d`
Non-interactive (silent) mode: • HBA compatibility scan and array software scan only • Report output directory—user-defined directory	`spcconfig -r -d --report-dir /mydir`

4. Type the `spcconfig` command you want to use, press **Enter** or **Return**, and follow the remaining installation prompts.

   Depending on which command options you specified, `spcconfig` prompts you for:

   - Report output directory—
     By default, `spcconfig` writes its SAN inventory report to the `spcconfig` installation directory which is:

     `/opt/VRTSspcfg/SunOS`

   - Use the matrix on the Web?—
     `spcconfig` can check the VERITAS Support Web site for a more recent version of the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* that `spcconfig` can use as it scans your hosts. The default is no.

   Note If your host does not have access to the Internet, see "Manually Updating the Compatibility List" on page 59.

   - Would you like to scan the network?—
     When run on a SANPoint Control QuickStart Server, `spcconfig` asks you if you want it to perform a SAN device compatibility scan—an SNMP (Simple Network

Management Protocol) sweep of one or subnets to determine if your SAN devices have compatible firmware. Device scans can only be specified when running `spcconfig` from a SANPoint Control QuickStart Server host, and can take several minutes on large networks. The default is yes.

Note `spcconfig` does not discover Cisco MDS switches that use SNMP v2x or v3.

- Would you like to scan different subnets?—
  If you specified `spcconfig` to perform a SAN device compatibility scan, `spcconfig` next asks you if you want to scan any subnets. The default is no.

  If you choose to scan subnets—
  Type the subnet and mask information using dot notation, separate them with a slash, and press **Enter** or **Return**.

  For example:

  `190.178.33.72/255.255.255.0`

  `10.68.29.5/255.255.255.0`

  Enter as many subnets as you want, delimiting them by pressing **Enter** or **Return**.

  Press **Enter** or **Return** twice in succession to indicate to `spcconfig` that you are finished entering subnets.

- Would you like to update `sal.conf` to enable out-of-band communication?—
  When run on a SANPoint Control QuickStart Server, `spcconfig` can update the QuickStart Server SAN discovery configuration file (`sal.conf`) with device IP addresses discovered during a device scan. Depending upon the type of SAN devices discovered, `spcconfig` updates the `sal.conf` out-of-band-related sections such as: `[MGEX]`, `[Exp.SNMP]`, `[Exp.Array]`, `[Exp.Bridge]`, and `[Exp.CiscoMDS]`. `spcconfig` backs up the configuration file prior to making modifications. In order for the `sal.conf` changes to take effect, `spcconfig` also restarts the SAL process on the host. The default is no.

When `spcconfig` is finished running, it will output a message similar to the following:

```
Script finished. Press enter key to continue.
```

5. Press **Enter** or **Return** to exit from `spcconfig`.

For more information about the `spcconfig` report, see "Viewing the SANPoint Control QuickStart Configuration Utility Report" on page 57.

Viewing the SANPoint Control QuickStart Configuration Utility Report

The SANPoint Control QuickStart Configuration Utility (`spcconfig`) generates and saves an inventory report of your SAN devices to the directory from which you ran `spcconfig`, or to the alternate directory you specified.

You can read the inventory report that `spcconfig` generates to see what devices, drivers, and related third-party software `spcconfig` detected on the host from which it was run. `spcconfig` hyperlinks the IP address for each device in the HTML version of the report, so you can view device information directly. You'll use this information to work through the configuration checklists located in "Device and Application Interoperability Requirement Checklists." These checklists will help you determine what changes you need to make to meet the requirements for SANPoint Control QuickStart and what SANPoint Control QuickStart features are available to you based on your configuration.

The report points out which devices are not configured correctly and offers corrective action recommendations. If the report does not list a device, that device is most likely a generic device (not listed in the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*) unless it is an HBA. A particular HBA may be supported, but if the driver is unsupported, `spcconfig` might not list it.

Tip When you run `spcconfig`, it can discover generic devices. Then, using SANPoint Control QuickStart you can enclose these generic devices and add attributes to them.

▼ To view the SANPoint Control QuickStart Configuration Utility report

1. `cd` to the directory where `spcconfig` saved the report files.

   The default is the directory from which you ran `spcconfig`.

2. Do one of the following:

   - Open *`host_dd_mm_yyyy_hh_mm_ss`*`.html` (where *host* is the name of the host on which you ran `spcconfig` and *dd_mm_yyyy_hh_mm_ss* stands for date and time) in a browser or other HTML viewer.
   - Open *`host_dd_mm_yyyy_hh_mm_ss`*`.csv` (where *host* is the name of the host on which you ran `spcconfig` and *dd_mm_yyyy_hh_mm_ss* stands for date and time) in a program such as `vi`, or a spreadsheet or database application that can read comma-separated values.

Note If you expected certain devices to show up on the list, check the latest *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*. The *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* is

available in PDF on the SANPoint Control CD (`spcqs_suptmx.pdf`). As SAN device vendor hardware and software information frequently changes, it is strongly recommended that you go to the VERITAS Support Web site to access the latest version of this document: http://seer.support.veritas.com/docs/260958.htm. If your host is without access to the Internet, see "Manually Updating the Compatibility List" on page 59.

Manually Updating the Compatibility List

The hardware and software compatibility list used by the SANPoint Control QuickStart Configuration Utility (`spcconfig`) to inventory your SAN can change between releases of SANPoint Control QuickStart. VERITAS may verify and add additional hardware, drivers, and firmware to the list supported by SANPoint Control QuickStart *after* the product ships.

If the host on which you are running `spcconfig` is connected to the Internet, `spcconfig` prompts you to automatically download the compatibility list and use it; however, if your SAN is running behind a firewall *without* access to the Internet, you must use a different method when you want to update the hardware and software compatibility list used by `spcconfig`.

This section describes how to manually update the compatibility list used by `spcconfig`.

Note This procedure assumes that you have root access on UNIX hosts or you are an administrator or a user in the Administrators group for Windows hosts.

▼ To manually update the compatibility list

1. On a host with Internet access, point a Web browser to the VERITAS Support Web site for SANPoint Control QuickStart:

   http://support.veritas.com/menu_ddProduct_SANPCTRL.htm

2. Click the **Downloads** link and locate the latest version of the compatibility list file for the version SANPoint Control QuickStart you are running.

   For example, the compatibility list file should be identified as something similar to the following:

   ```
   Utility -  Hardware list file (SpcQs_Compat_4_0) for the VERITAS
   SANPoint Control QuickStart 4.0 configuration utility
   ```

   The file itself should be named something similar to: `SpcQs_Compat_4_0_xxxxxx`

3. Download and save a copy of the compatibility list file.

4. Move the downloaded file to the following directory on the host on which you want to run `spcconfig`:

   ```
   /opt/VRTSspcs/spcconfig/Common/perl/lib
   ```

5. Make a backup copy of the existing compatibility list.

   For example:

   ```
   mv SpcQs_Compat_4_0 SpcQs_Compat_4_0.backup
   ```

6. Rename the latest compatibility list to:

   `SpcQs_Compat_4_0`

   For example:

   UNIX:

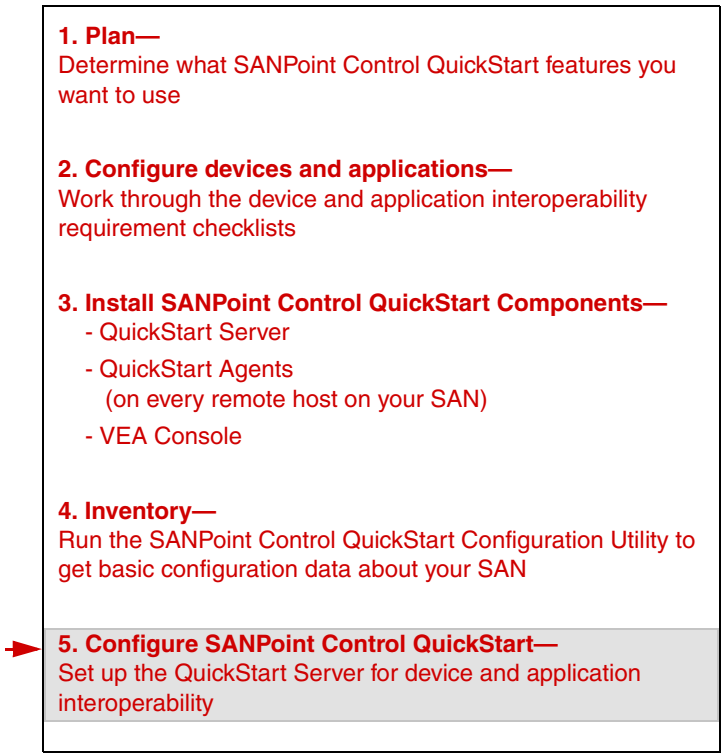
   ```
   mv SPC_Compat_3_6_xxxxxx SpcQs_Compat_4_0
   ```

For instructions on running `spcconfig`, refer to "Running the SANPoint Control QuickStart Configuration Utility" on page 53.

Configuring SANPoint Control QuickStart Discovery 5

This section provides information on how to configure SANPoint Control QuickStart for discovery of SAN devices and applications. Configuring for discovery is the last step in installing and configuring SANPoint Control QuickStart.

SANPoint Control QuickStart Installation and Configuration Flowchart



This section contains the following topics:

"Configuring SANPoint Control QuickStart Discovery Overview" on page 63

"Direct Attached Storage (DAS) Discovery Considerations" on page 65

"Configuring the Server for Agent Discovery" on page 66

"Configuring the Server for Cisco MDS Switch Discovery" on page 68
"Configuring the Server for Switch SNMP Discovery" on page 71
"Adding or Modifying Brocade Switch Credentials" on page 72
"Configuring the Server for Bridge and Router Discovery" on page 74
"Configuring the Oracle Explorer" on page 75
"Disabling CT Passthru" on page 77
"Configuring Discovery When Removing SAN Devices" on page 78

Configuring SANPoint Control QuickStart Discovery Overview

To configure SANPoint Control QuickStart for discovery, you must first ensure that your SAN devices and applications and their version, firmware, and so forth are supported by SANPoint Control QuickStart. VERITAS provides the SANPoint Control QuickStart Configuration Utility (`spcconfig`) to help you inventory your SAN and identify device incompatibilities. For more information, see "Getting Basic Configuration Data About Your SAN" on page 49.

SANPoint Control QuickStart Configuration Utility sweeps your SAN comparing your devices against the official SANPoint Control QuickStart-supported list referred to as the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* (http://seer.support.veritas.com/docs/260958.htm). If your devices use unsupported firmware versions, for example, then those devices will not be discovered properly and you will not get a complete or accurate picture of your SAN.

Your SAN devices and applications must be properly setup and configured. For example, if you want to do out-of-band discovery on a switch, the switch must be configured with the IP address of QuickStart Server, subnet mask, and gateway. This type of detailed configuration information is provided in the "Device and Application Interoperability Requirement Checklists" on page 7 manual.

Finally, you must ensure that the QuickStart Server and all QuickStart Agents are configured properly to discover and monitor devices on your SAN. The topics in this section explain how to do this.

▼ To configure SANPoint Control QuickStart discovery

1. Complete the configuration of your SAN devices by referring to "Device and Application Interoperability Requirement Checklists" on page 7.

2. Install the QuickStart Agent on every remote host in your SAN and configure the QuickStart Server for each Agent host to be discovered.

   For more information, see "Configuring the Server for Agent Discovery" on page 66.

3. Configure the SANPoint Control QuickStart Server for each Cisco switch to be discovered.

   For more information, see "Configuring the Server for Cisco MDS Switch Discovery" on page 68.

4. Configure the SANPoint Control QuickStart Server for each switch that you want to discover out-of-band using the SNMP explorer.

For more information, see “Configuring the Server for Switch SNMP Discovery” on page 71.

5. Configure the SANPoint Control QuickStart Server if your Brocade switches use non-default login credentials.

   For more information, see “Adding or Modifying Brocade Switch Credentials” on page 72

6. Configure the SANPoint Control QuickStart Server for each bridge or router to be discovered.

   For more information, see “Configuring the Server for Bridge and Router Discovery” on page 74.

7. If Oracle tablespaces are not being discovered, you may need to configure the Oracle explorer manually.

   For more information, see “Configuring the Oracle Explorer” on page 75.

8. If DB2 EE and EEE is being discovered, you must configure the DB2 explorer manually.

   For more information, see “vxDB2” on page 98.

Direct Attached Storage (DAS) Discovery Considerations

The following lists considerations for SANPoint Control QuickStart support of direct attached storage (DAS) discovery:

- SANPoint Control QuickStart discovers only SCSI disks. IDE disks are not discovered.
- You should see DAS disks in the VERITAS Enterprise Administrator (VEA) Console OS Handles pane under each host. If you look at the properties of the OS handle, it will show as **Direct-attached=True** and contain attributes for **DAS State** and **DAS Name**. Also, the Device Size should be populated.
- If the HBA explorer is disabled, or an unsupported HBA is found, then SAN-attached storage might show up as Direct Attached Storage.
- DAS enclosures, devices, and LUNs will display in the VERITAS Enterprise Administrator (VEA) Console Storage View only if they are fibre-attached in a point-to-point topology (no switches involved) to a host running the SANPoint Control QuickStart Agent with supported HBAs. Any SCSI bus-attached storage displays in the OS Handles pane only.
- SANPoint Control QuickStart visualizes VERITAS Volume Manager (volumes and disks) and VERITAS File System (disks) attached to SANPoint Control QuickStart Agent hosts.

Configuring the Server for Agent Discovery

The SANPoint Control QuickStart Server can discover information about HBAs on hosts that are attached to fabrics discovered by the QuickStart Server host. To get more detailed information about these hosts, you must install the SANPoint Control QuickStart Agent software on each host and register each Agent with the QuickStart Server. Additionally, if you want SAN discovery information from fabrics not attached to the QuickStart Server, you must install the QuickStart Agent software on at least one host in the remote fabric and specify it on the QuickStart Server to discover the fabric.

Within certain multi-fabric SAN configurations, it may be advisable to enable switch exploration on only one SANPoint Control Agent host for each fabric that is not attached to and thus not discovered by the QuickStart Server, while disabling switch exploration on other SANPoint Control Agent hosts. This will limit the amount of redundant traffic being generated by SANPoint Control explorers.

▼ To configure the QuickStart Server for QuickStart Agent host discovery

1. If you have not already done so, use the VERITAS Enterprise Administrator (VEA) Console to connect to the QuickStart Server on which you want your changes to take effect.

2. In the VEA Console, choose **Tools > SANPoint Control QuickStart > Configure Agent Hosts**.

   The Configure SANPoint Control QuickStart Agent Hosts dialog box displays.

3. In the Configure SANPoint Control QuickStart Agent Hosts dialog box, you can add QuickStart Agent hosts, in one of two ways:

   - Type each host name one at a time (step a)
   - Browse for one or more host names (step b)

   a. Select **Add New Host** to enter QuickStart Agent hosts one at a time. You can type the QuickStart Agent host name, qualified domain name, or IP address.

   b. Select **Browse for Hosts** to enter more than one SANPoint Control QuickStart Agent host at once and in the dialog box that displays, in the **Broadcast address** field, type in your SANPoint Control QuickStart Agent host search parameters and select **Refresh**. You can enter any of the following in this field:

      - IP address/host name—discover a particular SANPoint Control QuickStart Server.
      - Directed-broadcast address—an IP address used to discover SANPoint Control QuickStart Servers within a specific subnet. You can use any IP address in a subnet or a subnet mask.

- 255.255.255.255 (default)—a special IP address that discovers SANPoint Control QuickStart Servers within a subnet and which does not cross a subnet boundary.

Note When you select **Browse for Hosts**, SANPoint Control QuickStart sends a UDP broadcast message to discover any SANPoint Control QuickStart Agent hosts not initially displayed in the Configure SANPoint Control Agent Hosts dialog box.

In the **Available Hosts** list, click the remote hosts that you want to explore and then click the **Add** button. You can make multiple contiguous or noncontiguous selections in the list.

4. When adding QuickStart Agent hosts, you must decide whether to check the **Enable Switch Exploration** checkbox. (By default, switch exploration is disabled.)

   Enabling switch exploration causes the QuickStart Agent to run the Management Server explorer (MGEX). For each fabric, either the QuickStart Server or one QuickStart Agent should be performing in-band exploration via the MGEX explorer. Running the MGEX explorer from one host only per fabric will limit the amount of redundant traffic being generated by the MGEX explorer.

5. From the Configure SANPoint Control QuickStart Agent Hosts dialog box, to enable or disable switch exploration for a QuickStart Agent host in the list, select a host in the list, and then click the **Edit Host** button.

   a. In the Edit SANPoint Control QuickStart Agent Hosts dialog box, check or uncheck the **Enable Switch Exploration** checkbox.

   b. Click **OK**.

      The QuickStart Agent host is enabled or disabled for discovery and the dialog box closes. You should see your change displayed next to the QuickStart Agent host name or IP address in the list on the Configure SANPoint Control QuickStart Agent Hosts dialog box.

6. When you finish configuring QuickStart Agents in the Configure SANPoint Control QuickStart Agent Hosts dialog box, click **OK** to save your changes and to close the dialog box.

Configuring the Server for Cisco MDS Switch Discovery

To configure the Cisco MDS explorer, you specify switch names and SNMP information for each switch in the SANPoint Control QuickStart Server SAN discovery configuration file.

SANPoint Control QuickStart requires that you configure all your Cisco switches with the same set of SNMP v1, v2c, or v3 credentials. You can create multiple sets of credentials on the same Cisco MDS switch.

▼ To configure the QuickStart Server for Cisco MDS switch discovery

1. Open `sal.conf` in a text editor.

   `sal.conf` resides on the QuickStart Server host in `/var/VRTSspcq`

2. In the `[Exp.CiscoMDS]` section, locate the line containing the string:

   ```
   SwitchNameList =
   ```

3. If `SwitchNameList` is commented, remove the pound sign (#).

4. Type a valid name, qualified domain name, or IP address for your Cisco switch.

   If you are adding more than one, separate each entry with a semicolon (;). The maximum length for each line is 10,000 characters.

   For example:

   ```
   SwitchNameList=Switch3;Switch.myco.com;255.255.255.255
   ```

5. In the `[Exp.CiscoMDS]` section, locate and uncomment the line containing the string:

   ```
   SNMPVersion =
   ```

6. Type one of the following values to represent the SNMP version that you are using on your Cisco MDS switch or switches:

   `1`, **`2c`**, **`3`**

   For example:

   ```
   SNMPVersion = 1
   ```

7. If you are using SNMP version 1 or 2c, you can specify a community name by typing in the name in the following line. (Again, make sure that it is uncommented.) The community name *must* be read/write:

   ```
   SNMPCommunityName =
   ```

Note All Cisco switches using SNMP v1 and 2c must share the same SNMP read/write community name. On Cisco MDS switches, you can verify SNMP information by using the switch CLI command:
`show snmp`

For example:

```
SNMPCommunityName = public
```

8. If you are using SNMP version 3, then you must supply authentication and privacy values for the following lines:

Note SANPoint Control QuickStart requires that the SNMP v3 credentials for the switch be network-admin or some other role with read/write permissions. This network-admin account must be set up across all Cisco switches. On Cisco MDS switches, you can verify SNMP information by using the switch CLI command:
`show snmp`

- `SNMPSecurityLevel =`

  The possible values are:

  - **`noAuthNoPriv`**—No authentication and no privacy
  - **`authNoPriv`**—With authentication and no privacy
  - **`authPriv`**—With authentication and privacy

- `SNMPAuthProtocol =`

  Identifies authentication protocol used by the SNMP agent. The possible values are: **`MD5`** or **`SHA`**.

- `SNMPUserName =`

  Identifies the name of the user.

- `SNMPAuthPassPhrase =`

  Identifies password phrase used to authenticate the user. Required only if authentication is enforced.

- `SNMPPrivProtocol =`

  Identifies the privacy protocol used by the SNMP agent. Required only if privacy is enforced by the agent. The value must be **`DES`**.

- `SNMPPrivPassPhrase =`

  If security level indicates that privacy is enforced, this should identify the password phase used by the privacy protocol.

For more information, refer to “sal.conf” on page 102.

9. When you have finished editing `sal.conf` and have saved your changes, you must stop and restart the QuickStart Server for the changes to take effect.

   For information about stopping and restarting the QuickStart Server, see “Stopping and Starting SANPoint Control QuickStart” on page 84.

Configuring the Server for Switch SNMP Discovery

The SANPoint Control QuickStart Server is designed to do its exploration in-band across Fibre Channel; however there are certain circumstances in which you must enable out-of-band exploration using the SANPoint Control QuickStart SNMP explorer. When you have multiple McDATA switch fabrics, or if you use unsupported HBA drivers you should enable out-of-band exploration with the SNMP explorer.

This section describes how to configure the SNMP explorer for switch discovery.

▼ To configure the QuickStart Server for SNMP discovery

1. Open `sal.conf` in a text editor.

   `sal.conf` resides on the QuickStart Server host in `/var/VRTSspcq`

2. In the `[Exp.SNMP]` section, locate the line containing the string:

   ```
   SwitchNameList =
   ```

3. If `SwitchNameList` is commented, remove the pound sign (#).

4. Type a valid name, qualified domain name, or IP address for your switch.

   If you are adding more than one, separate each entry with a semicolon (;). The maximum length for each line is 10,000 characters.

   For example:

   ```
   SwitchNameList=Switch3;Switch.myco.com;255.255.255.255
   ```

Note For McDATA switches, enter the IP address for each McDATA proxy.

5. If your switch is a QLogic switch, enable `SCSI inquiry` and `drvconfig`. Locate the [`HBA`] section. Verify that the following lines are present and not commented:

   ```
   Disable_scsi_inquiry = 0
   ```

   ```
   Disable_drvconfig = 0
   ```

   For more information, refer to "sal.conf" on page 102.

6. When you have finished editing `sal.conf` and have saved your changes, you must stop and restart the QuickStart Server for the changes to take effect.

   For information about stopping and restarting the QuickStart Server, see "Stopping and Starting SANPoint Control QuickStart" on page 84.

Adding or Modifying Brocade Switch Credentials

If your Brocade switches use non-default login credentials (a username that is not `admin` and a password that is not `password`) then you must configure the SANPoint Control QuickStart Server with the Brocade credentials. The section describes how to add or modify login credentials for Brocade switches and QuickLoops (virtual hubs) requiring an administrative login for a SAN Access Layer (SAL) explorer to log in to the switch.

▼ To add or modify Brocade switch credentials on a SANPoint Control QuickStart Server host

1. On the SANPoint Control QuickStart Server host, open a Solaris console and log in as `root`.

2. Open `sal.conf` in a text editor.

   By default, `sal.conf` resides in the following location:

   `/var/VRTSspcq`

3. Locate the any pre-existing switch credentials, in order to group the credential entries in one part of `sal.conf`. If there are no credentials, locate the `[Sample.Switch.Credentials]` section.

4. Type the following:

   `[Switch:`*`switchName`*`]`

   `Login=`*`switchUser`*

   `Password=`*`switchPassword`*

   `Shared=0 | 1`

Note SANPoint Control QuickStart ignores lines in `sal.conf` that begin with `#`.

For out-of-band MGEX exploration, the *switchName* must match the switch name used earlier in the `SwitchNameList` of the `[MGEX]` section of `sal.conf`.

For in-band exploration and out-of-band SNMP exploration, the *switchName* must be the switch name, the switch World Wide Name (WWN), or switch IP address.

You can specify more than one *switchName* by delimiting each with a semi-colon (;). The number of switches is limited by the line length supported by `sal.conf` (10,000 characters). For out-of-band MGEX exploration, *switchName* can be an [MGEX] `SwitchNameList` entry.

switchUser is a valid username for switches requiring an administrative login for a SAL explorer to log in to the switch.

switchPassword is a valid password for switches requiring an administrative login for a SAL explorer to log in to the switch.

When `Shared` is on (`Shared=1`) the switch credentials are shared by all switches in the same fabric containing the referenced switch. The default is off (`Shared=0`). This entry is used by the fabric traversal code and not by MGEX out-of-band exploration. If set to 1, then the switch credentials will be migrated to all switch objects in the same fabric as the referenced switch (unless they have their own switch credentials section).

Note After switch credentials have been migrated into the store, there is no way to remove them besides deleting the switch object. While changing the switch credentials in `sal.conf` will result in the switch credentials being changed in the store, removing switch credentials from `sal.conf` will not result in switch credentials being removed from the switch objects themselves. Returning a switch to the default credentials requires that the switch credentials either be changed to the default values or that the switch object be deleted (after the credentials have been removed from `sal.conf`).

5. When you have finished editing `sal.conf` and have saved your changes, you must stop and restart the SAN Access Layer for the changes to take effect.

   For information about stopping and restarting the QuickStart Server, see "Stopping and Starting SANPoint Control QuickStart" on page 84.

Configuring the Server for Bridge and Router Discovery

The SANPoint Control QuickStart Server's SAN Access Layer (SAL) is designed to explore your SAN in-band across Fibre Channel. To discover bridges and routers, however, you must configure the QuickStart Server's Bridge explorer to utilize out-of-band discovery.

▼ To configure the QuickStart Server for bridge and router discovery

1. Open `sal.conf` in a text editor.

   `sal.conf` resides on the QuickStart Server host in `/var/VRTSspcq`

2. In the `[Exp.Bridge]` section, locate the line containing the string:

   ```
   SNMPNameList=
   ```

3. If `SNMPNameList` is commented, remove the pound sign (#).

4. Type a valid name, qualified domain name, or IP address for your bridge or router.

   If you are adding more than one, separate each entry with a semicolon (;). The maximum length for each line is 10,000 characters.

   For example:

   ```
   SNMPNameList=Bridge1;Router.myco.com;255.255.255.255
   ```

5. Refer to "sal.conf" on page 102 for more information, especially if your bridge or router:

   - Is discovered in-band via a device node
   - Uses an SNMP community name other than public
   - Is an iSCSI router that uses a port other than 5003

6. When you have finished editing `sal.conf` and have saved your changes, you must stop and restart the QuickStart Server for the changes to take effect.

   For information about stopping and restarting the QuickStart Server, see "Stopping and Starting SANPoint Control QuickStart" on page 84.

Configuring the Oracle Explorer

The SANPoint Control QuickStart Oracle explorer supports Oracle database discovery. The explorer discovers Oracle tablespaces and files, and their correlation to volumes and LUNs on a SAN for the following Oracle versions: 8.x, 8i, and 9i.

In most cases the SANPoint Control QuickStart Oracle explorer discovers Oracle instances automatically, but if Oracle tablespaces are not being discovered, you may need to configure the explorer manually. To configure the Oracle explorer manually, you must run a configuration script on each host running Oracle. The script, `vxOra`, is in the same directory as the executable `vxsald`.

Note SANPoint Control QuickStart still performs nominal discovery of Oracle attributes even if the script is not run.

You will be prompted to configure Oracle discovery during installation. In most cases this is not necessary as the explorer will be configured automatically. Choosing "yes" at that time will run the configuration script described previously.

The `vxOra` script will ask for the following information: Instance Name, Oracle Home, an Oracle account (that must have access to v$ and dba views), and the password for this account. (The password will be encrypted before writing to file.) When the script is run it generates a configuration file, `vxOra.conf`. This file is used by the SAN Access Layer to connect to Oracle instances for discovery/exploration. Note that you can monitor as many instances as are running on a host. You can also disable or enable discovery of any of the instances at any time by running `vxOra`. The script allows you to add, modify, delete and disable the discovery of Oracle instances.

In most cases, the Oracle explorer will configure itself automatically. Use the following instructions to configure the explorer manually in the event that the automatic configuration fails.

▼ To configure the SANPoint Control QuickStart Oracle explorer

1. Change to the SANPoint Control QuickStart directory on your QuickStart Server or QuickStart Agent host:

   `cd /opt/VRTSsal`

2. At the command prompt, type the following and press **Enter** or **Return**:

   `./vxOra`

3. Add an Oracle instance:

   a. Type **a**

   b. Enter the value for ORACLE_SID (Oracle Instance Name)

   c. Enter the value for ORACLE_HOME path

   d. Enter the value for USER (Oracle account that must have access to v$ and dba views)

   e. Enter the value for PASSWORD

   f. Re-enter the value for PASSWORD

4. Delete an Oracle instance:

   a. Type **d**

   b. Type the Oracle Instance Name

5. Modify an Oracle instance:

   a. Type **m**

   b. Enter the value for ORACLE_SID (Oracle Instance Name)

   c. Enter the value for ORACLE_HOME path

   d. Enter the value for USER (Oracle account that must have access to v$ and dba views)

   e. Enter the value for PASSWORD

   f. Re-enter the value for PASSWORD

6. To quit, type **q**

Disabling CT Passthru

If the HBA or HBA driver on your SANPoint Control QuickStart Server or SANPoint Control QuickStart Agent host does not support Common Transport (CT) operations, you might need to disable the MGEX explorer from using Fibre Channel connections via the CT protocol.

Disabling CT passthru on the SANPoint Control QuickStart Server does *not* affect instances of the MGEX explorer running on SANPoint Control QuickStart Agent hosts. (SANPoint Control QuickStart Agent hosts running MGEX are declared under `InBandHosts` in the `[Remote]` section of `sal.conf` on the SANPoint Control QuickStart Server.) If you want to disable CT passthru for a SANPoint Control QuickStart Agent, you must disable it on the SANPoint Control QuickStart Agent host itself.

▼ To disable the MGEX explorer from using in-band operations

1. Open the SANPoint Control QuickStart Server configuration file `sal.conf` in a text editor:
   - On the SANPoint Control QuickStart Server, `sal.conf` resides by default in: `/var/VRTSspcq`
   - On SANPoint Control QuickStart Servers configured to be highly available with VERITAS Cluster Server:
     - There is a soft link to `sal.conf` to `/var/VRTSspcq/sal.conf`
     - Also, open the SAL configuration file for the agent mode. The configuration file resides by default in: `/opt/VRTSsal/sal/.salr.conf.ha`
   - On SANPoint Control QuickStart Agents, `sal.conf` resides by default in `/opt/VRTSsal`
2. In `sal.conf`, locate the `[MGEX]` section.
3. Type in the following:

   `DisableCT=1`

Note SANPoint Control QuickStart ignores lines in `sal.conf` that begin with the pound sign (#).

4. When you finish editing `sal.conf`, save your changes, and then stop and restart the SANPoint Control QuickStart Server' SAN Access Layer (SAL) for the changes to take effect.

   For more information about stopping and restarting the SAN Access Layer, see "vxsal" on page 131.

Configuring Discovery When Removing SAN Devices

After you have initially configured the SANPoint Control QuickStart Server for discovery, if you remove a device from your SAN, you might need to reconfigure your discovery settings.

▼ To reconfigure the QuickStart Server for discovery when SAN devices are removed

- If the device you are removing is a SANPoint Control QuickStart Agent, remove the Agent host list of Agent hosts for the SANPoint Control QuickStart Server to discover.

  You do this in the VERITAS Enterprise Administrator (VEA) Console in the SANPoint Control Agent Hosts dialog box (**Tools > SANPoint Control QuickStart > Configure Agent Hosts**).

Note You might also want to uninstall the QuickStart Agent on that host. For more information, see "Uninstalling SANPoint Control QuickStart" on page 87).

- If the device you are removing is a Cisco MDS switch, remove or unregister it from the QuickStart Server. For information, see "Removing Cisco MDS Switches from Discovery" on page 79.

- If the device you are removing is a switch that you are discovering out-of-band using the SNMP explorer, remove or unregister it from the QuickStart Server. For information, see "Removing Switches Discovered With the SNMP Explorer" on page 80.

- If the device you are removing is a bridge or a router, remove or unregister it from the QuickStart Server. For information, see "Removing Bridges and Routers from Discovery" on page 81.

Removing Cisco MDS Switches from Discovery

Whenever you remove a Cisco MDS switch from your SAN, you should also remove the entry for that switch in the list of Cisco MDS switches to be discovered on the QuickStart Server.

▼ To remove Cisco MDS switches from discovery

1. Open `sal.conf` in a text editor.

   `sal.conf` resides on the QuickStart Server host in `/var/VRTSspcq`

2. In the `[Exp.CiscoMDS]` section, locate the line containing the string:

   ```
   SwitchNameList =
   ```

3. Remove the switch name or switch IP address from the `SwitchNameList` line.

4. When you have finished editing `sal.conf` and have saved your changes, you must stop and restart the QuickStart Server for the changes to take effect.

   For information about stopping and restarting the QuickStart Server, see "Stopping and Starting SANPoint Control QuickStart" on page 84.

Removing Switches Discovered With the SNMP Explorer

Whenever you remove a switch being discovered by the SNMP explorer from your SAN, you should also remove its entry in the SNMP explorer list on the QuickStart Server.

▼ To remove switches from SNMP explorer discovery

1. Open `sal.conf` in a text editor.

   `sal.conf` resides on the QuickStart Server host in `/var/VRTSspcq`

2. In the `[Exp.SNMP]` section, locate the line starting with the following string:

   ```
   SwitchNameList =
   ```

3. Remove the switch name or switch IP address from the `SwitchNameList` line.

Note For McDATA switches, remove the IP address for each McDATA proxy.

   For more information, refer to "sal.conf" on page 102.

4. When you have finished editing `sal.conf` and have saved your changes, you must stop and restart the QuickStart Server for the changes to take effect.

   For information about stopping and restarting the QuickStart Server, see "Stopping and Starting SANPoint Control QuickStart" on page 84.

Removing Bridges and Routers from Discovery

To maintain your SAN, you might have to remove a bridge or router. In removing the bridge or router, you might also want to disable out-of-band exploration via the SANPoint Control QuickStart Server's Bridge explorer. This will prevent the QuickStart Server from trying to discover and manage the bridge or router in the future.

▼ To remove bridges and routers from discovery

1. Open `sal.conf` in a text editor.

   `sal.conf` resides on the QuickStart Server host in `/var/VRTSspcq`

2. In the `[Exp.Bridge]` section, locate the line containing the string:

   `SNMPNameList=`

3. Remove the bridge or router name or IP address from the `SNMPNameList` line.

4. When you have finished editing `sal.conf` and have saved your changes, you must stop and restart the QuickStart Server for the changes to take effect.

   For information about stopping and restarting the QuickStart Server, see "Stopping and Starting SANPoint Control QuickStart" on page 84.

Running SANPoint Control QuickStart 6

After you configure the SAN discovery configuration file (`sal.conf`), you must restart the SANPoint Control QuickStart Server. To use the VERITAS Enterprise Administrator (VEA) Console, you must connect to a QuickStart Server. This section describes how to perform both of these tasks:

"Stopping and Starting SANPoint Control QuickStart" on page 84

"Connecting to the SANPoint Control QuickStart Server" on page 85

Stopping and Starting SANPoint Control QuickStart

By default, the SANPoint Control QuickStart Server and the SANPoint Control QuickStart Agent are configured at installation to start when you boot up your Server and your Agent hosts. If you need to stop and restart either the Server or the Agent, follow the steps in this section.

▼ To stop or to restart SANPoint Control QuickStart

1. Change to the SANPoint Control QuickStart directory on your QuickStart Server or QuickStart Agent host:

   `cd /opt/VRTSsal`

   Tip SANPoint Control QuickStart creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. To avoid having to change to the SANPoint Control QuickStart directory, add `/opt/VRTS/bin` to your host's `PATH` environment variable to access the SANPoint Control QuickStart scripts and commands.

2. At the command prompt, type the following and press Enter or Return:

   `./vxsal stop`

   Tip You can also stop and restart the SANPoint Control QuickStart with: `vxsal restart`

   On Server hosts this stops the QuickStart Server; on Agent hosts, this stops the QuickStart Agent.

   Note After stopping SANPoint Control QuickStart daemons, wait about thirty seconds before starting them again. This gives the operating system time to free up logical ports and other resources that the SANPoint Control QuickStart processes need upon restart.

3. At the command prompt, type the following and press Enter or Return:

   `./vxsal start`

   On Server hosts the command restarts the QuickStart Server; on Agent hosts, the command restarts the QuickStart Agent.

Connecting to the SANPoint Control QuickStart Server

You must run the VERITAS Enterprise Administrator (VEA) Console and connect to the SANPoint Control QuickStart Server to use SANPoint Control QuickStart. This section describes how to connect to a QuickStart Server from a Solaris and a Windows VEA Console. All SANPoint Control QuickStart users have administrator-level permissions.

▼ To connect to the SANPoint Control QuickStart Server on Solaris

1. Change to the VERITAS Enterprise Administrator (VEA) Console directory, by typing the following command and then pressing Enter or Return:

   `cd /opt/VRTob/bin`

   Tip SANPoint Control QuickStart creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. To avoid having to change to the VEA directory, add `/opt/VRTS/bin` to your host's `PATH` environment variable to access the SANPoint Control QuickStart scripts and commands.

2. Start the VEA Console by typing the following command and then pressing **`Enter`** or **`Return`**:

   `./vea`

   Note You can also run the VEA Console in the background by typing: **`./vea&`**

   The VERITAS Enterprise Administrator (VEA) Console launches. Upon startup, the Connection dialog box displays.

3. Supply the data in the following fields and then click **OK**:

   - **Hostname—**
     Type the name, IP address, or qualified domain name for QuickStart Server host.
   - **Username—**
     Type **`root`**.

   Note The login credentials for the SANPoint Control QuickStart Server are identical to the QuickStart Server host Solaris root credentials, **`root`** and its password. See your system administrator for more information.

   - **Password—**
     Type the password for the Solaris `root` account on the QuickStart Server.

   You are now connected to your SANPoint Control QuickStart Server.

For information on how to use the VERITAS Enterprise Administrator (VEA) Console, refer to the manual, *SANPoint Control QuickStart Overview Guide*.

▼ To connect to the SANPoint Control QuickStart Server on Windows

1. From the Windows **Start** menu, choose the shortcut to run the VEA Console. The default shortcut is **Programs > VERITAS Enterprise Administrator** .

   The VERITAS Enterprise Administrator (VEA) Console launches. Upon startup, the Connection dialog box displays.

2. Supply the data in the following fields and then click **OK**:

   - **Hostname—**
     Type the name, IP address, or qualified domain name for QuickStart Server host.
   - **Username—**
     Type **`root`**.

   Note The login credentials for the SANPoint Control QuickStart Server are identical to the QuickStart Server host Solaris root credentials, **`root`** and its password. See your system administrator for more information.

   - **Password—**
     Type the password for the Solaris `root` account on the QuickStart Server.

   You are now connected to your SANPoint Control QuickStart Server.

For information on how to use the VERITAS Enterprise Administrator (VEA) Console, refer to the manual, *SANPoint Control QuickStart Overview Guide*.

Uninstalling SANPoint Control QuickStart 7

This section contains the following topics:

"Uninstalling SANPoint Control QuickStart" on page 88

"Uninstalling the VERITAS Enterprise Administrator (VEA) Console" on page 90

Uninstalling SANPoint Control QuickStart

This section describes how to run the SANPoint Control QuickStart Uninstall Script to uninstall the SANPoint Control QuickStart (both the Server and the Agent) on a Solaris host.

▼ To uninstall SANPoint Control QuickStart

1. Log on as root.
2. Mount VERITAS Storage Solutions software disc 2.
3. Change to the `sanpoint_control_quickstart` directory.
4. Type the following command and press Enter or Return:

   `./uninstallspcq`

   The SANPoint Control QuickStart install script prompts you with the name of the hosts on which you want to uninstall the QuickStart Server.

   ```
   Enter the system names separated by spaces on which to uninstall
   SPCQ:
   ```

5. Type the name, IP address, or fully qualified domain name of the host on which you want to uninstall the QuickStart Server and press Enter or Return.

   The SANPoint Control QuickStart install script checks the system to determine if other installed VERITAS products have a dependency on any packages you are removing. If there are any such dependencies, the affected packages are left on the system and not marked for removal.

   ```
   Leaving VRTSob installed on myServer due to its package
   dependencies: VRTSmuobg
   ```

   The SANPoint Control QuickStart install script confirms that you want to uninstall the QuickStart Server and its dependencies.

   ```
   uninstallspcq is now ready to uninstall SPCQ packages.
   All SPCQ processes that are currently running will be stopped.

   Are you sure you want to uninstall SPCQ packages? [y,n,q] (y)
   ```

6. Type **`y`** and press Enter or Return to remove the SANPoint Control QuickStart Server.

   The SANPoint Control QuickStart Uninstall Script removes SANPoint Control QuickStart and its dependencies. The script displays a message similar to the following when complete:

```
Uninstallation of SANPoint Control QuickStart has completed
successfully.
```

Uninstalling the VERITAS Enterprise Administrator (VEA) Console

This section describes how to remove the VERITAS Enterprise Administrator (VEA) Console from a Solaris and a Windows host.

▼ To uninstall the VEA Console on Solaris

1. Log on to the Solaris host as root.
2. uninstall `VRTSobgui`, by typing the following command and press Enter or Return:

   `pkgrm VRTSobgui`
3. Follow the `pkgadd` prompts.

   For more information, consult your Solaris manual pages for `pkgadd`.

▼ To uninstall the VEA Console on Windows

1. Log on to the Windows host as a user with Administrator privileges.
2. In the Windows Control Panel, double-click **Add/Remove Programs**.

   The Add/Remove Programs Properties dialog box displays.
3. Select **VERITAS Enterprise Adminstrator** from the list of currently installed programs.
4. Select **Change/Remove**, and follow the remaining panels in the Wizard.

Command and Configuration File Reference A

SANPoint Control QuickStart provides commands that you can run from a UNIX shell, as well as configuration files that are integral to its operation.

This section contains the following topics:

"Commands and Configuration Files Locator" on page 92

"spcconfig" on page 93

"vxDB2" on page 98

"vxOra" on page 100

"sal.conf" on page 102

"vxsal" on page 131

"vxsald" on page 133

Commands and Configuration Files Locator

SANPoint Control QuickStart creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to access the SANPoint Control QuickStart scripts and commands.

The table below maps the SANPoint Control QuickStart command/configuration file with its respective SANPoint Control QuickStart host and default installation directory:

SANPoint Control QuickStart Commands and Configuration Files Locations

This Command or Configuration File...	... Can Be Accessed on This Host... ... At This Default Location
"sal.conf"	QuickStart Server: `/var/VRTSspcq` QuickStart Agent: `/opt/VRTSsal`
"spcconfig"	QuickStart Server and QuickStart Agent: `/opt/VRTSspcfg/SunOS`
"vxDB2"	QuickStart Server and QuickStart Agent: `/opt/VRTSsal`
"vxOra"	QuickStart Server and QuickStart Agent: `/opt/VRTSsal`
"vxsal"	QuickStart Server and QuickStart Agent: `/opt/VRTSsal`
"vxsald"	QuickStart Server and QuickStart Agent: `/opt/VRTSsal`

spcconfig

NAME

spcconfig - inventories your SAN to configure the SANPoint Control Server for discovery

SYNOPSIS

```
spcconfig [ [-d] | [-d -r] | [-d -u] | [-u] | [-r] ]
          [--report-dir][--use-web-matrix] | [-h | -v]
```

DESCRIPTION

`spcconfig` is the SANPoint Control QuickStart Configuration Utility, a program that inventories your SAN to automatically configure the SANPoint Control QuickStart Server for discovery. If you want to configure your SANPoint Control QuickStart Server manually, `spcconfig` also generates a configuration report. (See "NOTES" later in this section for more information on the configuration report.)

When you run `spcconfig`, it performs the following:

- HBA compatibility scan—sweeps the local host (a SANPoint Control QuickStart Server or Agent) for HBA drivers to compare them against the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*.

Depending upon the options you specify, `spcconfig` can perform the following on a SANPoint Control QuickStart Server host:

- SAN device compatibility scan—performs an SNMP (Simple Network Management Protocol) sweep of one or subnets to determine if your SAN devices have compatible firmware. Device scans can only be specified when running `spcconfig` from a SANPoint Control QuickStart Server host, and can take several minutes on large networks.

  Note `spcconfig` does not discover Cisco MDS switches that use SNMP v2x or v3.

- Enabling out-of-band communication—when run on a SANPoint Control QuickStart Server host, `spcconfig` can update the QuickStart Server's SAN discovery configuration file (`sal.conf`) with device IP addresses discovered during a device scan to enable out-of-band communication mechanisms. Depending upon the type of SAN devices discovered, `spcconfig` updates the `sal.conf` out-of-band-related sections such as: `[MGEX]`, `[Exp.SNMP]`, `[Exp.Array]`, `[Exp.Bridge]`, and `[Exp.CiscoMDS]`. `spcconfig` backs up the configuration file prior to making modifications. In order for the `sal.conf` changes to take effect, `spcconfig` also restarts the SAN Access Layer (SAL) process on the host.

OPTIONS

`-d`

(For SANPoint Control QuickStart Server hosts only.) Run `spcconfig` in non-interactive mode with default values for user-input prompts. `-d` detects HBA drivers, scans for third-party array management software, and sweeps the network for SAN devices.

When you specify `-d`, `spcconfig` uses the following default values for these user-input prompts:

Report output directory—`spcconfig` installation directory. (See "NOTES" later in this section.)

Use the matrix on the Web?—no

Would you like to scan the network?—yes

Would you like to scan different subnets?— no

Would you like to update sal.conf to enable out-of-band communication?— no

Tip You can combine `-d` with other options to stay in non-interactive mode while picking and choosing which default values to override. See "EXAMPLES" later in this section for some ideas.

`-r`

(For Solaris and Windows 2000 hosts only.) Causes `spcconfig` to scan the local host for HBA drivers and third-party array management software and compares them against the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* . On other operating systems, `-r` is the default and cannot be overriden.

`-r` cannot be used with `-u`.

`-u`

Commit the results of the SAN device scan to the SANPoint Control QuickStart Server SAN discovery configuration file (`sal.conf`) for out-of-band SAN communication and create a backup copy in the same directory.

`-u` cannot be used with `-r`.

For more information, see "sal.conf" on page 102.

`--report-dir` *`directory`*

Directory in which `spcconfig` writes its SAN inventory report files. *directory* is a valid directory on the local host on which `spcconfig` is running. (`--report-dir` is case-sensitive.)

When `--report-dir` is *not* specified and running in interactive mode, `spcconfig` prompts you for a report directory. The default report directory is contingent on whether SANPoint Control QuickStart is

already installed. If SANPoint Control QuickStart is installed, the default report directory is the `spcconfig` installation directory; otherwise, the default directory is the current directory. (See "NOTES" later in this section.)

`--use-web-matrix`

Force `spcconfig` to go to the VERITAS Support Web site to download and use the latest *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* when scanning your SAN for supported devices. (`--use-web-matrix` is case-sensitive.)

If your host is without access to the Internet, see "Manually Updating the Compatibility List" on page 59.

`-h`

Display the list of `spcconfig` options and a brief description for each.

`-v`

Display the version of `spcconfig`.

NOTES

On both SANPoint Control QuickStart Server and Agent hosts, `spcconfig` resides by default in: `/opt/VRTSspcfg/SunOS`

SANPoint Control QuickStart creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to access the SANPoint Control QuickStart scripts and commands.

To run `spcconfig` you must have root privileges on Solaris. For step-by-step instructions on how to run `spcconfig`, refer to "Running the SANPoint Control QuickStart Configuration Utility" on page 53

You should run `spcconfig` on every host on your SAN. You can save time (and avoid a subnet scan) by using the `-r` option on Solaris hosts on which you have installed (or plan to install) SANPoint Control QuickStart Agents.

When you want to scan additional subnets, type the name of each subnet on separate lines delineated by a carriage return. After typing the last subnet, enter two successive carriage returns to notify `spcconfig` that you are finished.

When you run `spcconfig` with the `-u` option on the SANPoint Control QuickStart Server host, `spcconfig` automatically updates the SANPoint Control QuickStart Server SAN discovery configuration file (`sal.conf`) with the necessary device and proxy IP addresses. You still must manually specify QuickStart Agents in the `sal.conf [Remotes]` section. For more information, see "Configuring the Server for Agent Discovery" on page 66.

The report `spcconfig` creates is available both as an HTML file and a comma-separated value (CSV) file and resides in the directory from which you ran `spcconfig` or the directory you specified. `spcconfig` names the reports:

- *`host_dd_mm_yyyy_hh_mm_ss`*.html
- *`host_dd_mm_yyyy_hh_mm_ss`*.csv

(where *host* is the name of the host on which you ran `spcconfig` and *dd_mm_yyyy_hh_mm_ss* stands for date and time.)

The report points out which devices are not configured correctly and offers corrective action recommendations. If the report does not list a device, that device is most likely a generic device (not listed in the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*) unless it is an HBA. A particular HBA may be supported, but if the driver is not, it might not be listed. Verify any missing SAN objects in your Configuration Report with the latest *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* available on the VERITAS Support Web site at: http://seer.support.veritas.com/docs/260958.htm. If your host is without access to the Internet, see "Manually Updating the Compatibility List" on page 59.

When you run `spcconfig` on a SANPoint Control QuickStart Server host with the `-u` option, (or if you choose to enable out-of-band communication during an interactive session), `spcconfig` writes IP-related SAN device information to `sal.conf` and creates a backup copy in the same directory named:

`sal.conf_`*`dd_mm_yyyy_hh_mm_ss`*

EXAMPLES

EXAMPLE 1: The following example shows how to run `spcconfig` in interactive mode. `spcconfig` prompts you for the information described earlier. (See "-d" earlier in this section.)

```
spcconfig
```

`spcconfig` will prompt you for a SAN device compatibility scan and whether to update the SANPoint Control QuickStart Server SAN configuration file for out-of-band communication; on other supported operating system hosts, `spcconfig` performs HBA compatibility and array software scans only.

EXAMPLE 2: The following example shows how to run `spcconfig` in non-interactive mode and—when run on the SANPoint Control QuickStart Server host—automatically update the QuickStart Server SAN discovery configuration file, `sal.conf`, for out-of-band-communication. (See "DESCRIPTION" earlier in this section.) Here, `spcconfig` uses default values (see "-d" earlier in this section) except that it will write its SAN inventory report to a user-specified directory (`/mydir`):

```
spcconfig -d -u --report-dir /mydir
```

EXAMPLE 3: The following example shows how to run `spcconfig` interactively to avoid scanning the network for SAN devices and perform only an HBA compatibility and an array software scan:

```
spcconfig -r
```

EXAMPLE 4: The following example shows how to run `spcconfig` non-interactively to perform an HBA compatibility scan only and to avoid scanning the network for SAN devices and perform only an HBA compatibility and an array software scan:

```
spcconfig -d -r
```

SEE ALSO

"vxDB2" on page 98

"vxOra" on page 100

"sal.conf" on page 102

"vxsal" on page 131

vxDB2

NAME

vxDB2 - invokes the interactive configuration script required to run the SANPoint Control QuickStart DB2 explorer

SYNOPSIS

```
vxDB2
```

DESCRIPTION

`vxDB2` invokes the interactive configuration script required to run the SANPoint Control QuickStart DB2 explorer. The vxDB2 explorer discovers IBM DB2 instances, databases, tablespaces, containers, files, and correlates them to volumes and LUNs in your SAN.

OPTIONS

After you have started a vxDB2 interactive session, you can type one of the following options:

`a`

Add one or more DB2 instances to the list of DB2 instances being discovered by the SANPoint Control QuickStart DB2 explorer.

`m`

Edit the discovery configuration for one or more DB2 instances being explored by the SANPoint Control QuickStart DB2 explorer.

`d`

Remove one or more DB2 instances from the list of DB2 instances being discovered by the SANPoint Control QuickStart DB2 explorer.

`q`

Exit `vxDB2`.

NOTES

To enable DB2 discovery, you must run `vxDB2` on each participating host. Although the SANPoint Control QuickStart install script, gives you an opportunity to run `vxDB2`, you can run `vxDB2` at any time to change configuration for the vxDB2 explorer.

`vxDB2` collects information about DB2 instance name, DB2 instance home directory, DB2 instance owner (user) name and password. `vxDB2` generates a configuration file (`vxDB2.conf`) used by the SAN Access Layer (`vxsald`) to connect to each DB2 instance for discovery. You can disable or enable discovery of any single DB2 instance at any time by running `vxDB2`, as `vxDB2` enables you to add, modify, delete, and disable exploration of one or more DB2 instances.

On the QuickStart Server and Agent, `vxDB2` and the file in which it stores configuration data (`vxDB2.conf`) reside by default in `/opt/VRTSsal`

SANPoint Control QuickStart creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to access the SANPoint Control QuickStart scripts and commands.

To run `vxDB2` on a QuickStart Server or QuickStart Agent host, you must be logged in as root.

SEE ALSO

"sal.conf" on page 102

"spcconfig" on page 93

"vxOra" on page 100

"vxsal" on page 131

vxOra

NAME

vxOra - invokes the interactive configuration script optionally required to run the SANPoint Control QuickStart Oracle explorer

SYNOPSIS

```
vxOra
```

DESCRIPTION

`vxOra` invokes the interactive configuration script optionally required to run the SANPoint Control QuickStart Oracle explorer.

OPTIONS

After you have started a vxOra interactive session, you can type one of the following options:

`a`

Add one or more Oracle instances to the list of Oracle instances being discovered by the SANPoint Control QuickStart Oracle explorer.

`m`

Edit the discovery configuration for one or more Oracle instances being explored by the SANPoint Control QuickStart Oracle explorer.

`d`

Remove one or more Oracle instances from the list of Oracle instances being discovered by the SANPoint Control QuickStart Oracle explorer.

`q`

Exit `vxOra`.

NOTES

On the QuickStart Server and Agent, vxOra resides in `/opt/VRTSsal`

SANPoint Control QuickStart creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to access the SANPoint Control QuickStart scripts and commands.

To enable Oracle discovery (which includes discovery of tablespaces, files, and correlating them to volumes and LUNs in SAN), an interactive configuration script (`vxOra`) sometimes must be run on each participating host.

To run `vxOra` on a SANPoint Control QuickStart Agent host, you must be logged in as `root`.

During installation, SANPoint Control QuickStart attempts to automatically gather Oracle configuration information, in order for the Oracle explorer to automatically run without intervention. However, there are some situations in which Oracle auto configuration is impossible. `vxOra` should be run when:

- When the DBA connects to Oracle as `internal` and is prompted for a password.
- On HP-UX remote hosts when active Oracle instances are not listed in the Oracle configuration file (`/etc/oratab`, by default).

If the SANPoint Control QuickStart installation script detects any of the above conditions, you are prompted to configure the Oracle explorer during installation; however, SANPoint Control QuickStart enables you to configure the Oracle explorer at any time by running `vxOra`.

`vxOra` collects information about `OracleSid` (`InstanceName`) and `OracleHome`, an Oracle account that must have access to the `v$` and `dba` views. `vxOra` generates a configuration file (`vxOra.conf`) used by the SAN Access Layer (`vxsald`) to connect to each Oracle instance for discovery. You can disable or enable discovery of any single Oracle instance at any time by running `vxOra`, as `vxOra` enables you to add, modify, delete, and disable exploration of one or more Oracle instances.

SEE ALSO

"spcconfig" on page 93

"sal.conf" on page 102

"vxsal" on page 131

sal.conf

Note Some information herein applies to the full SANPoint Control product only. A comprehensive list of platforms and SAN devices supported by SANPoint Control QuickStart is available in the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* at: http://seer.support.veritas.com/docs/260958.htm

NAME

sal.conf - configuration file for SAL primaries and SAL remotes

SYNOPSIS

```
{{[Section] parameter}...}
```

DESCRIPTION

`sal.conf` is the configuration file for the SAN Access Layer (SAL) daemon/service—`vxsald`. Entries in this file are for use on the SAL primary only, unless identified for use on a SAL remote.

[STORE]

`Path=`*pathName*

`sal pkgadd` dictates where the store is installed. If *pathName* does not point to an an existing, writable directory one will be created. `sal pkgadd` updates this variable to be the installer specified location. Store files and directory are created automatically when SAL is first run.

[AGENT]

`Port=`*portNumber*

The port on which the agent (SAL primary) listens for client connections. `Port` is also the port that SAL remotes use to send data from remote explorers to the SAL primary. For SANPoint Control QuickStart, VERITAS Software has reserved port 2802 (the default) with IANA (Internet Assigned Numbers Authority). *portNumber* can only be changed for the primary SAL. SAL remotes always use the registered port, 2802.

`Compression=1 | 0`

1 = ON; 0 = OFF (default).

Compression controls whether or not SAL compresses its responses to a client (such as the VEA Console or `vxsalcmd`). If `Compression = 1` and the client request indicates that the client supports compression

(HTTP header for the request contains: "Accept-Encoding: gzip"), then SAL compresses the client response. If `Compression = 0` or is omitted, SAL disables compression. By default, compression is disabled.

`Authentication=1 | 0`

1 = ON (default); 0 = OFF.

Determines whether a user name and password are required for client requests. When authentication is turned on, the user name and password are validated before the connection to the SAL primary is made. Three types of users are supported:

- admin—Has the ability to create/modify SAL users as well as view/modify the SAN configuration
- readonly—Allows a user to only view SAN configuration information but does not permit changes
- readwrite—Allows users to view and change the SAN configuration; for example: add attributes and perform zoning operations.

`PortRange=`*PortLow-PortHigh*

Defines a range of outgoing ports. The outgoing port for SAL primary to SAL remote is assigned from this range. If not defined, the next available port is assigned dynamically.

`AuditLog =` *pathName*

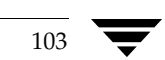
The SAN Access Layer (SAL) logs the requests made of it by the clients (clients could include the following: SANPoint Control QuickStart Console, SANPoint Control QuickStart Web Console, and CLIs) in the Audit log. By default, the Audit log is written to a log file (`auditlog`) that resides in `/var/VRTSspcs` (UNIX) and `\Program Files\Veritas\SANPoint Control\SPC Data` (Windows). You can change the name of this file and its path. If you specify a path that does not exist, SAL creates the directory structure and the specified file. If `AuditLog` is omitted, SAL disables it by default.

`MaxAuditLogSize =` *n*

Specifies the maximum audit log size (in MB), which is 10 MB by default. When the size of the audit log exceeds `MaxAuditLogSize` bytes, all auditing information beyond the minimum number of days of auditing information to retain (`MinAuditLogDays`) will be removed from the Audit log and archived. Up to 10 audit archive files (with file extensions `.`*N*`.gz`, where *N* is 0-9) will be retained.

`MinAuditLogDays =` *n*

Specifies the minimum number of days of auditing information to retain in the Audit log, which is 30 days by default.



SAL does not archive the Audit log until both the retention time and maximum file size parameters are met. Once the maximum file size is met, SAL hourly checks the Audit log to determine whether the retention days parameter has been met. If so, SAL only removes those days beyond the minimum number of days from the Audit log and archives them.

[SSL]

By default, SAL allows anonymous SSL connections between a client (for example a SANPoint Control QuickStart Console, SANPoint Control QuickStart Web Console, and CLIs) and SAL. You can disable anonymous SSL connections and require SAL to use a certificate file and a private key to authenticate its SSL connections.

`Anonymous = 1 | 0`

1 = YES (default); 0 = NO

Determines whether anonymous (Diffie-Hellman) SSL is enabled. This allows use of SSL without certificates and private keys. By default, anonymous SSL is enabled.

`CertificateFile =` *certificateFilename*

certificateFilename specifies the name of the file containing the SSL certificate (in PEM format). If the certificate file is specified but the private key file is not, both certificate and private key must be stored in the certificate file.

`PrivateKeyFile =` *privateKeyFilename*

privateKeyFilename specifies the name of the file containing the SSL private key (in PEM format). If the certificate file is specified but the private key file is not, both certificate and private key must be stored in the certificate file.

[REMOTE]

On a SAL primary, defines SAL remote hosts that are explored by the SAL explorers running on the SAL remote hosts.

On a SAL remote, defines authorized SAL primaries that the SAL remote host accepts requests from.

`Hosts=`*hostName*

On a SAL primary, `Hosts` defines SAL remote hosts that are explored by all SAL explorers running on the SAL remote hosts, except MGEX. The remote explorers include MGEX, HBA, Array, VM, VCS, NBU, NBUAPP, Exchange, Oracle, and DB2 remote explorers.

If the remote SAL server is unavailable, or if it is not specified correctly, the primary SAL will periodically attempt communication and will timeout. Timeouts are noted in the `syslog`.

hostName can be either a hostname, IP address, or a fully qualified domain name. For example: `myHostName`, `0.0.0.0`, or `myhost.domain.com`

Individual host entries are separated by a semicolon (;). For example:

```
host = host1;host2;host3
```

You can have multiple lines of host names, where the second entry (`myhost.xyzabc.com`) is on a separate line. For example:

```
host=10.212.10.89
host=myhost.xyzabc.com
```

`InBandHosts=`*hostName*

On a SAL primary, `InBandHosts` defines the remote SAL hosts that are explored by all SAL explorers running on the SAL remote hosts, including MGEX. The remote explorers include MGEX, HBA, Array, VM, VCS, NBU, Exchange, Oracle, and DB2 remote explorers.

Any fabric that is not explored by a primary SAL should be explored by one remote SAL running both MGEX (inband) and the remote explorers. Include this remote SAL in the `InBandHosts` entry. See preceding section for *hostName* description. A fabric should be explored by only one explorer running on one host (primary or remote).

The difference between the `Hosts` and `InBandHosts` entries is that remotes specified in `InBandHosts` run all remote explorers while remotes specified in `Hosts` run all remote explorers except MGEX. Most remote hosts will be listed in Hosts.

`Primary =` *primaryName*

On a SAL remote, specifies the primary SALs that are allowed to make requests of the remote explorers. The default value is null. If this entry is omitted or null, the SAL remote accepts only discovery requests from all SAL primaries; the remote does not accept management requests from any primaries. If this entry contains an asterisk (*), discovery and management requests are accepted from all SAL primaries. If primary SALs are specified, requests for discovery or management are accepted from only those listed primaries.

If the primary is running on a port other than 2802, the port number must also be specified using the format `host:port`.

primaryName can be either a hostname, IP address, or a fully qualified domain name. For example: `myPrimaryName`, `0.0.0.0`, or `myprimary.domain.com`

Individual host entries are separated by a semicolon (;). For example:

```
Primary = primary1;primary2;primary3
```

`AllowMinimalResponses = 1 | 0`

1 = ON (default); 0 = OFF.

If `AllowMinimalResponses = 1` (default), remote hosts are allowed to send short "nothing changed" responses to the primary SAL. Otherwise, remote hosts may not send these responses. `AllowMinimalResponses` can be used to enhance performance when multiple remotes are managed by a primary SAL. Disabling `AllowMinimalResponses` has a negative impact on performance.

`disable = 1 | 0`

1=ON; 0=OFF(default

To disable all remote explorers, set `disable = 1`.

[LOG]

`LogSpec=`*`pathName`*

Defines private log parameters that can be specified on SAL remotes and SAL primaries.

pathName can be any valid path and filename. If you specify a path that does not exist, SAL creates the directory structure and the specified file.

The default value is: `/var/log/vxsaldlog` (UNIX) or `%systemdrive%\Program Files\Veritas\SANPoint Control\SPC Data\vxsald.log` (Windows).

`Size=`*`n`*

n is a number representing the maximum size of the private log file in megabytes (MB).

`UseSyslog = 1 | 0`

1 = ON (default); 0 = OFF.

On a primary or a remote SAL, if the private log file is not defined, SAL evaluates `UseSyslog`.

If a private log file is defined for logging (`LogSpec=`*`pathName`*), SAL ignores `UseSyslog`— even when its value is defined as `1` in `sal.conf`.

When `UseSyslog` is evaluated, if `UseSyslog = 1`, SAL logs to the host system log. If `UseSyslog = 0`, SAL does not log to the host system log.

SAL uses any configurations (such as debug level) set in the the system log's configuration file. (On UNIX, this configuration file resides in `/etc/syslog.conf`).

[EXPLORERS]

`Delay=`*n*

On a SAL primary or a SAL remote, this is the wait interval between explorations. The valid values for *n* are 10–86400 seconds for the exploration wait interval. The default value is 90 seconds on a SAL primary. The default value is null on a SAL remote. If the value on a SAL remote is null, 0, or if `Delay` is missing, the remote explorers perform explorations only when requested by the primary. If `Delay` is specified on a remote, changes require at least that amount of time to be discovered.

`Delay` is overriden for the Array Management explorer by the `SessionInterval` parameter in "[Exp.Array]" on page 113.

`Delay` can be overriden for the Oracle explorer by assigning a wait interval value to the `ExplorationInterval` parameter in "[Exp.ORA]" on page 111.

`Delay` can be overriden for the DB2 explorer by assigning a wait interval value to the `ExplorationInterval` parameter in "[Exp.DB2]" on page 111.

[MGEX]

Configures the GS-3 Management Server Explorer (MGEX). MGEX uses the Fibre Channel Common Transport (CT) protocol to discover switches in-band over Fibre Channel, to obtain switch characteristics, and to explore port connectivity. MGEX applies to all switches that are physically connected and that are capable of communicating in-band. However, `SwitchNameList` applies only to Brocade Communication switches.

MGEX can optionally run over any IP network to discover Brocade fabrics. The MGEX Explorer also performs McData, QLOGIC, INRANGE, and Cisco zoning (in-band).

Use the `[MGEX] SwitchNameList` entry only in situations where the hosts attached to Brocade switches either have no HBA card or use an unsupported card/firmware version. If this situation applies to your configuration, you should list one or two of the Brocade Communications switches within each Fabric that they are part of. (You can use just one switch, but by listing two, you gain some redundancy in case of problems with a single switch).

If you are able to discover all fabrics using in-band exploration using HBA cards, this entry is not needed. However, it may be used even if you do have HBA based in-band capability, by listing a Brocade switch for each fabric, to provide redundant communication paths at the expense of somewhat more processing usage.

For more information, see the administrator or user guide for your product.

`SwitchNameList=`*switchAddress*`[;`*switchAddress*`][;...]`

SwitchNameList is used on SAL primaries only. *switchAddress* can be either a switchname, IP address, or a fully qualified domain name.

Note If your Brocade switch uses logon credentials, then its `SwitchNameList` entry and its *switchName* in its credentials entry must match the switch's DNS entry.

You can specify more than one *switchAddress* by delimiting each with a semi-colon (;). The number of switches is limited by the line length supported by `sal.conf` (10,000 characters).

If the switch is unavailable, exploration of the switch fails and an error is logged to `syslog`.

`VerifyVendor=1 | 0`

1 = TRUE (verify); 0 = FALSE (do not verify) (default)

On SAL primaries and remotes, verifies vendor OIDs within World Wide Names. `0` (default) disables `VerifyVendor`. `VerifyVendor` works for both in-band and out-of-band explorations.

`Disable=1 | 0`

1 = TRUE (DISABLED); 0 = FALSE (ENABLED) (default)

Disables/enables the MGEX explorer on primary SALs and remote SALs. The MGEX explorer is enabled by default.

`CiscoMDSExplorationDisable=1 | 0`

1 = TRUE (DISABLED) (default); 0 = FALSE (ENABLED)

Disables/enables Cisco MDS exploration through MGEX. Cisco MDS switch exploration is disabled by default. If commented out or not defined, switch exploration is disabled. If you are using the Cisco MDS explorer (see "[Exp.CISCOMDS]" on page 128) to explore Cisco switches, insure that `CiscoMDSExplorationDisable=1` to avoid conflicts with the Cisco MDS explorer. If you have Cisco MDS switches that cannot be discovered by the Cisco MDS explorer (if, for example, they are behind a firewall), set `CiscoMDSExplorationDisable=0` to explore those switches.

`CiscoMDSZoningDisable=1 | 0`

1 =TRUE (DISABLED) (default); 0 =FALSE (ENABLED)

Disables/enables Cisco MDS zoning through MGEX. Cisco MDS switch zoning is disabled by default. If commented out or not defined, switch zoning is disabled. If you are using the Cisco MDS explorer (see "[Exp.CISCOMDS]" on page 128) to explore Cisco switches, insure that `CiscoMDSZoningDisable=1` to avoid conflicts with the Cisco MDS

explorer. If you have Cisco MDS switches that cannot be discovered by the Cisco MDS explorer (if, for example, they are behind a firewall), set `CiscoMDSMDSZoningDisable=0` to enable zoning of those switches.

`DisableCT=1 | 0`

1 = TRUE (DISABLED); 0 = FALSE (ENABLED) (default)

Disables/enables in-band CT passthrough commands on remote SAL. This is used to stop in-band CT passthrough commands from being sent through unstable HBAs.

[ZONING]

This section configures SAL to discover zones.

For more information, see the administrator or user guide for your product.

`Disable=1 | 0`

1 = ON; 0 = OFF (default).

Disables/enables all SAL zoning. The Zoning explorer is enabled by default.

[HBA]

This section configures the HBA (host bus adapter) explorer and requires root privileges. The HBA explorer discovers host, LDDL, and HBA information.

For more information, see the administrator or user guide for your product.

`Disable=1 | 0`

1 = ON; 0 = OFF (default).

Disables/enables the HBA explorer on primary SAL and remote SAL. The HBA explorer is enabled by default.

`Disable_hba_discovery = 1 | 0`

1 = ON; 0 = OFF (default).

Enables or disables only HBA discovery on primary SAL and remote SAL. `Disable_hba_discovery` does *not* affect host and LDDL discovery. HBA discovery is enabled by default.

Disable HBA discovery to avoid log messages stating that you do not have privilege to access the HBA, if running the QuickStart Server without root privilege.

`Disable_scsi_inquiry=1 | 0`

1 = ON; 0 = OFF (default).

On primary SAL and remote SAL, disables/enables SCSI inquiries of target devices.

`Set_scsi_timeout=` *n*

On primary SAL and remote SAL, *n* is the timeout interval in seconds. (Default is five seconds.)

`Disable_drvconfig=1 | 0`

1 = ON; 0 = OFF (default).

On primary SAL and remote SAL, disables/enables drvconfig execution in the HBA explorer.

`Immediate_drvconfig = 1 | 0`

0 = OFF; 1 = ON (default).

On primary SAL and remote SAL, disables/enables the HBA explorer running `drvconfig` immediately after a zoning command.

`drvconfig_delay =` *n*

Specifies delay (in seconds) that the HBA explorer always waits before issuing `drvconfig`. The default is five seconds.

`hba_cache_timeout =` *n*

On SAL primaries and SAL remotes, specifies the HBA explorer cache refresh interval in minutes. The default value = 5 minutes; setting n = 0 disables automatic cache refresh.

The HBA explorer caches discovery information. The cache information is updated at the interval specified by the `hba_cache_timeout` value and whenever a zoning or LUN masking operation occurs.

On Microsoft Windows machines, VERITAS NetBackup cannot run if the cache is being updated. If you install NetBackup on a Microsoft Windows machine where the HBA explorer is running, set `hba_cache_timeout = 0` to disable automatic cache updates.

[EXP.VM]

This section configures VERITAS Volume Manager (UNIX) and VERITAS Storage Foundation for Windows (Windows) exploration.

For more information, see the administrator or user guide for your product.

`Disable=1 | 0`

0 = OFF (default); 1 = ON.

On SAL primaries running on UNIX or Microsoft Windows systems, disables/enables exploration of VERITAS Volume Manager and VERITAS Storage Foundation for Windows. On SAL remotes running on Microsoft Windows systems, disables/enables exploration of Storage Foundation for Windows. The explorer is enabled by default.

`VMForcedDiscoveryVersion = Volume Manager` *`versionNumber`*

On SAL primaries and SAL remotes running on Windows hosts only, specifies the VERITAS Storage Foundation for Windows version to be discovered. If commented out or not defined, the default is version 2.7 or 3.1. This enables discovery of future versions of Storage Foundation for windows.

`versionNumber` is the VERITAS Storage Foundation for Windows version defined in the Windows Registry.

[EXP.ORA]

This section configures Oracle exploration (UNIX only) on remote and primary SAL.

For more information, see the administrator or user guide for your product.

`Disable = 1 | 0`

0 = OFF (default); 1 = ON.

Disables/enables explorer. The Oracle explorer is enabled by default.

`DisableVxMSLoading = 1 | 0`

1 = ON; 0 = OFF (default).

Disables/enables file to LUN mapping of Oracle files. By default, file to LUN mapping of Oracle files is enabled.

`ExplorationInterval = n`

The time, in seconds, between explorations for Oracle applications. The default value specified in `sal.conf` is 3600 seconds. If a value is not specified, the default exploration interval value, `Delay`, in "[Explorers]" on page 107 is used.

`AutoDiscover = 1 | 0`

1 = auto-discovery enabled (default); 0 = auto-discovery disabled

Enables/disables automatic Oracle discovery.

`DisableBlockSizeAttributes = 1 | 0`

1 = disable (default); 0 = enable

Disables/enables discovery of block size attributes for Oracle discovery. Discovery of the `BlockReads` and `BlockWrites` attributes in the `Table` object and the `PhysicalBlockReads` and `PhysicalBlockWrites` attributes in the `File` object are disabled/enabled.

[EXP.DB2]

This section configures DB2 exploration. The DB2 explorer runs on Solaris primary and remote SAL hosts and on AIX remote SAL hosts.

For more information, see the administrator or user guide for your product.

`Disable = 1 | 0`

0 = OFF (default); 1 = ON.

Disables/enables explorer. The DB2 explorer is enabled by default.

`DisableVxMSLoading = 1 | 0`

1 = ON; 0 = OFF (default).

Disables/enables file to LUN mapping of DB2 files. By default, file to LUN mapping of DB2 files is enabled.

`ExplorationInterval = n`

The time, in seconds, between explorations for DB2 applications. *n* is set to 3600 seconds (1 hour) in the `sal.conf` file; you can modify this value. If a value is not specified, the default exploration interval value, `Delay`, in "[Explorers]" on page 107 is used.

[EXP.SNMP]

This section configures SNMP (Simple Network Management Protocol) exploration. If there is no (uncommented) *SwitchNameList* in the EXP.SNMP section, then SAL disables this explorer. SNMP exploration is not done on SAL remotes.

For more information, see the administrator or user guide for your product.

`Disable=1 | 0`

1 = ON; 0 = OFF (default).

Disables/enables SNMP exploration. The SNMP explorer is enabled by default.

`FabricElement_MIB=1 | 0`

1 = ON (default); 0 = OFF.

By default, SNMP does not discover switches with the Fabric Element MIB. Setting `FabricElement_MIB` to `1` enables Fabric Element MIB exploration (currently, Brocade Communication switches only).

`SwitchNameList=`*switchAddress*`[;`*switchAddress*`][;...]`

switchAddress can be either a switchname, IP address, or a fully qualified domain name.

You can specify more than one *switchAddress* by delimiting each with a semi-colon (;). The number of switches is limited by the line length supported by `sal.conf` (10,000 characters).

If the switch is unavailable, exploration of the switch fails and an error is logged to `syslog`.

[EXP.SNMPTRAP]

This section enables/disables SAL from listening for incoming SNMP traps.

`Disable=1 | 0`

1 = ON (default); 0 = OFF.

Enables/disables SAL from listening for incoming SNMP traps. The SNMP Trap explorer is disabled by default.

[EXP.ARRAY]

This section configures disk array exploration. The Array Management explorer, which runs on SAL primary and SAL remote hosts, discovers and manages in-band and out-of-band disk arrays. Out-of-band arrays are explored by the SAL primary; in-band arrays can be explored by SAL primary or SAL remote hosts. However, it is recommended that you connect storage arrays that are managed in-band to a SAL remote host rather than the SAL primary. For a complete list of arrays that are supported by your product, refer to the product HCL.

The Array Management explorer also discovers and manages Virtual Enclosures in Cisco MDS 9000 Family switches. The Virtual Enclosures are created and managed by VERITAS Network Volume Manager *for Cisco*. Virtual Enclosures are analogous to storage arrays that are discovered and managed out-of-band. Storage associated with Virtual Enclosures can be allocated to hosts similar to the way that storage in a disk array can be allocated to hosts. For more information, see the documentation that comes with the Cisco MDS 9000 Family switch and the documentation that comes with VERITAS Network Volume Manager *for Cisco*.

Configuration information is put in this section to enable discovery and management of:

- storage arrays that are managed out-of-band
- Virtual Enclosures in Cisco MDS switches

Arrays that are managed in-band do not require configuration.

Some storage arrays are managed through a management appliance or server, which can control more than one storage array. For storage arrays that are managed by a management appliance or server, configure information for the management appliance or server not for the individual storage arrays. See "SUPPORTED OUT-OF-BAND STORAGE ARRAYS" on page 116 for more information.

`Disable=1 | 0`

1 = ON; 0 = OFF (default).

Disables/enables the Array Management explorer. The Array Management explorer is enabled by default.

`SessionInterval = n`

Specifies how often, in seconds, arrays and Virtual Enclosures are polled during exploration cycles. Overrides the explorer delay for array exploration. On the SAL primary, the default value is 615 seconds (non-multiple of the other explorer delays in order to normalize CPU

usage). On the SAL remote, the default value is 0, which means that the array explorer only performs explorations when requested by the primary.

`ArrayNameList=`*arrayAddress*`|`*arrayManagerAddress*`[;`*arrayAddress*`|`*arrayManagerAddress*`][;...]`

To explore out-of-band storage arrays, place the host names or IP addresses of the arrays or management appliances or servers in `ArrayNameList`. To explore Virtual Enclosures in Cisco MDS switches, place the names or IP addresses of the hosts where VERITAS Network Volume Manager *for Cisco* server is running in `ArrayNameList`. *arrayAddress* (*arrayManagerAddress)* can be either a disk array (or management appliance or server, or Network Volume Manager server host) name, IP address, or a fully qualified domain name. For example:

`ArrayNameList = myFirstArray; mySecondArray; 10.1.1.1`

You can specify more than one *arrayAddress* or *arrayManagerAddress* by delimiting each with a semi-colon (;). The number of arrays, array managers, and Network Volume Manager server hosts is limited by the line length supported by `sal.conf` (10,000 characters).

If the array, management appliance, or Network Volume Manager server host is unavailable, exploration fails and an error is logged to `syslog`.

`[Array:` *arrayAddress*`|`*arrayManagerAddress*`]`

When exploring disk arrays or Virtual Enclosures in Cisco MDS switches out-of-band, provide an array credentials/configuration section for each array, array management appliance or server, or Network Volume Manager server host specified in `ArrayNameList`. *arrayAddress* and *arrayManagerAddress* are defined in `ArrayNameList` above.

Some storage arrays have a management appliance or server that manages one or more arrays. In that case, enter the host name or IP address of the management appliance or server rather than the individual storage arrays.

arrayAddress and *arrayManagerAddress* must exactly match what is defined in ArrayNameList. For example, you cannot declare **`myArray`** in the `ArrayNameList` and **`myArray.company.com`** in the `[Array: ]` section.

`IPAddr =` *arrayIPAddress*

If you specified the name, rather than the IP address, in the `ArrayNameList` but want to use the IP address to access the array, array manager, or Network Volume Manager server host, specifiy the IP address with `IPAddr`.

`Login =` ***arrayUser*** | ***arrayManagerUser***

When exploring storage arrays and Virtual Enclosures out-of-band, provide a valid username (***arrayUser*** or ***arrayManagerUser***) for the Array explorer to log on to the storage array, management appliance, or Network Volume Manager server host.

Note `Login` can contain a null value (`Login=`) if username configuration is not required.

`Password =` ***arrayPassword*** | ***arrayManagerPassword***

When exploring storage arrays and Virtual Enclosures out-of-band, provide a valid password (***arrayPassword*** or ***arrayManagerPassword***) for the Array explorer to log on to the array, management appliance, or Network Volume Manager server host. When SAL first reads the password from `sal.conf`, SAL encrypts the password, places the password in another file, and replaces the password in `sal.conf` with asterisks (*).

Note `Password` can contain a null value (`Password=`) if password configuration is not required.

`Model =` ***arrayModel*** | ***arrayManagerModel***

When exploring storage arrays and Virtual Enclosures out-of-band, provide a valid array model (***arrayModel***), management appliance model (***arrayManagerModel***), or Virtual Enclosure model (***arrayModel***). The following are valid model values:

hp_512 or hp_xp_512

hp_eva

emc_clariion

hds_9910

hds_9960

hds_9900, which can be used instead of hds_9910 or hds_9960

hicommand

sun_t3+ or sun_t300

ibm_shark

nec_istorage

cisco_mds

`Provider =` ***arrayProvider***

Instead of specifying a storage array, management appliance, or Virtual Enclosure model, you can specify the provider that manages it. This enables support of additional storage array models that can be managed

by existing providers. If you specify a `Model` and a `Provider`, the `Provider` value overrides the `Model` value. The following are valid provider values:

vx_hp_512

vx_hp_eva

vx_emc_clariion

vx_hds_9900

vx_hicommand

vx_sun_t300

vx_ibmshark

vx_nec_istorage

vx_cisco_mds

`ScanInterval = n`

Specifies how often storage arrays or Virtual Enclosures are re-scanned to learn of any state changes.

n is a number that represents minutes. The default value is 30 minutes. Do not change this value unless you need a longer polling interval.

`ServerPort = serverPortValue`

Specify this value if you are entering configuration information for a Hitachi HiCommand server. *serverPortValue* specifies the port that the HiCommand provider uses to communicate with the HiCommand server, which manages Hitachi storage arrays. See "SUPPORTED OUT-OF-BAND STORAGE ARRAYS" for information about which arrays are managed by the HiCommand server.

There can be more than one HiCommand server, each managing more than one storage array.

If you do not specify a port, the default of 2001 is used.

`OptionalParams = optionalParams`

Some storage arrays use additional configuration information. Specify the same value as the setting in the storage array. For example:

```
OptionalParams = public
```

SUPPORTED OUT-OF-BAND STORAGE ARRAYS

As of initial product release, SAL supports the following out-of-band storage arrays, which are configured in the Array section. See the HCL and Release Notes that come with your product for information about which storage arrays are supported by the product and for information about any additional supported storage arrays.

Hewlett-Packard XP48 and XP512

Model = hp_512 | hp_xp_512

Provider = vx_hp_512

For configuration information, see "EXAMPLE 1" on page 119.

Hewlett-Packard StorageWorks Enterprise Virtual Array (HP EVA)

Model = hp_eva

Provider = vx_hp_eva

These arrays are managed through the HP OpenView Storage Management Appliance (Management Appliance). Enter configuration information for the Management Appliance, not the individual HP EVA arrays. The IP address or name used must match the *arrayManagerAddress* specified in the `ArrayNameList`.

For configuration information, see "EXAMPLE 2" on page 119.

EMC CLARiiON FC4700 and CX6000

Model = emc_clariion

Provider - vx_emc_clariion

Each CLARiiON storage array can have up to two Storage Processors. Each Storage Processor has its own IP address and name. When you configure information for an array, specify one of the IP addresses or names. The IP address or name used must match the *arrayAddress* specified in the `ArrayNameList`.

For configuration information, see "EXAMPLE 3" on page 120.

Model = hds_9910 or hds_9960 or hds_9900, which applies to both array models

Provider = vx_hds_9900

For configuration information, see "EXAMPLE 4" on page 120.

If you are using the Hitachi HiCommand server to manage other Hitachi arrays, do not configure these individual arrays. (For HiCommand server configuration information, see "EXAMPLE 5" on page 120.)

Model = hicommand

Provider = vx_hicommand

Do not configure each individual array. Instead, insure that these storage arrays have a network connection to the HiCommand server and configure the HiCommand server for management instead of the individual arrays. The IP address or name used must match the *arrayManagerAddress* specified in the `ArrayNameList` for the Hitachi HiCommandServer.

For configuration information, see "EXAMPLE 5" on page 120.

Sun StoreEdge T3 and T3+ Storage Arrays

Model = sun_t3+, for the Sun T3B, or sun_t300, for the Sun T300

Provider = vx_sun_t300

For configuration information, see "EXAMPLE 6" on page 121.

IBM TotalStorage Enterprise Storage Server (IBM ESS/IBM Shark) IBM ESS 800 and IBM ESS 10/20

Model = ibm_shark

Provider = vx_ibmshark

These arrays are managed by the IBM ESS Specialist, which is installed in the storage array. You can have one Specialist manage one storage array or you can manage more than one array through a single Specialist. If you are managing more than one array through a single Specialist, configure that Specialist only; do not configure the individual arrays. The IP address or name used must match the *arrayManagerAddress* specified in the `ArrayNameList` for the ESS Specialist.

For configuration information, see "EXAMPLE 7" on page 121.

NEC Storage Series Disk Arrays/iStorage S Series

This out-of-band storage array is supported, but does not require any configuration information.

Model = nec_istorage

Provider = vx_nec_istorage

Virtual Enclosures in Cisco MDS Switches

Model = cisco_mds

Provider = vx_cisco_mds

Network Volume Manager creates and manages Virtual Enclosures, which are analogous to storage arrays, in Cisco MDS switches. Enter configuration information for each host where Network Volume Manager server is running.

For configuration information, see "EXAMPLE 8" on page 122.

CONFIGURATION EXAMPLES FOR OUT-OF-BAND STORAGE ARRAYS

The examples in this section show only the required parameters for each storage array, array management appliance or server, and Virtual Enclosures. In the array configuration/credentials section, you can optionally specify `IPAddr` or `ScanInterval`. Instead of specifying `Model`, you can specify `Provider`.

EXAMPLE 1

Hewlett-Packard XP48 and XP512

These storage arrays require the following configuration information. ***arrayAddress*** must match the ***arrayAddress*** specified in the `ArrayNameList`:

Array Address

Model or Provider

OptionalParams - value of SNMP Read Community and SNMP Write Community in the storage array

Configuration:

```
[Array:arrayAddress]
model=hp_512
OptionalParams = public
```

EXAMPLE 2

Hewlett-Packard StorageWorks Enterprise Virtual Array (HP EVA)

These arrays are managed through the HP OpenView Storage Management Appliance (Management Appliance). Enter the following configuration information for the Management Appliance, not the individual HP EVA arrays. ***arrayManagerAddress*** must match the ***arrayManagerAddress*** specified in the `ArrayNameList`:

Array Manager Address

Login - user name to log on to the Management Appliance

Password - password to log on to the Management Appliance

Model or Provider, where Model is the model name of the Management Appliance and Provider is the name of the provider that manages the Management Appliance

Configuration:

```
[Array:arrayManagerAddress]
login= managementApplianceUser
password=managementAppliancePassword
model=hp_eva
```

EXAMPLE 3

EMC CLARiiON FC4700 and CX6000

Each CLARiiON storage array can have up to two Storage Processors. Each Storage Processor has its own IP address and name. When you configure information for the array, specify one of the IP addresses or names for *arrayAddress*. The IP address or name used must match the *arrayAddress* specified in the `ArrayNameList`. These storage arrays require the following configuration information:

Array Address

Model or Provider

Configuration:

```
[Array:arrayAddress]
model=emc_clariion
```

EXAMPLE 4

If you are using the Hitachi HiCommand server to manage other Hitachi arrays, do not configure these individual arrays. Instead, insure that these storage arrays have a network connection to the HiCommand server and configure the HiCommand server for management instead of the individual arrays (See "EXAMPLE 5"). *arrayAddress* must match the *arrayAddress* specified in the `ArrayNameList`:

Array Address

Model or Provider

OptionalParams - value of SNMP Read Community and SNMP Write Community in the storage array

Configuration:

```
[Array:arrayAddress]
model=hds_9900
OptionalParams = public
```

EXAMPLE 5

These arrays are managed through the HiCommand server. Do not configure each individual array. Instead, insure that these storage arrays have a network connection to the HiCommand server and configure the HiCommand server for management instead of the individual arrays. Configure the following parameters for the HiCommand server. If

there is more than one HiCommand server, enter information for each Server. *arrayManagerAddress* must match the *arrayManagerAddress* specified in the `ArrayNameList`:

Array Manager Address

Login

Password

Model or Provider, where Model is the model name of the HiCommand server and Provider is the name of the provider that manages the HiCommand server

ServerPort - optional. If not specified the default port of 2001 is used.

Configuration:

```
[Array:arrayManagerAddress]
login= managementApplianceUser
password=managementAppliancePassword
model=hicommand
```

EXAMPLE 6

Sun StoreEdge T3 and T3+ Storage Arrays

These storage arrays require the following configuration information. *arrayAddress* must match the *arrayAddress* specified in the `ArrayNameList`:

Array Address

Login

Password

Model or Provider

Configuration:

```
[Array:arrayAddress]
login= arrayUser
password=arrayPassword
model=sun_t3+
```

EXAMPLE 7

IBM TotalStorage Enterprise Storage Server (IBM ESS/IBM Shark) IBM ESS 800 and IBM ESS 10/20

These arrays are managed by the IBM ESS Specialist, which can be installed in each storage array. You can have one Specialist manage one storage array or you can manage more than one array through a single Specialist. If you are managing more than one array through a single Specialist, configure that Specialist only; do not configure the individual arrays.

Configure the following parameters for each ESS Specialist that is managing an array. *arrayManagerAddress* must match the *arrayManagerAddress* specified in the `ArrayNameList`:

Array Manager Address - IP address or name of the ESS Specialist

Login - user name to log on to the ESS Specialist

Password - password to log on to the ESS Specialist

Model or Provider, where Model is the model name of the ESS Specialist and Provider is the name of the provider that manages the ESS Specialist

Configuration:

```
[Array:arrayManagerAddress]
login= managementApplianceUser
password=managementAppliancePassword
model=ibm_shark
```

EXAMPLE 8

Virtual Enclosures in Cisco MDS Switches

Network Volume Manager creates and manages Virtual Enclosures in Cisco MDS switches. To discover and manage Virtual Enclosures, configure the following parameters for each host where Network Volume Manager server is running:

Array Address - the IP address or name of the host where Network Volume Manager server is running

Login - user name to log on to the Network Volume Manager server host

Password - password to log on to the Network Volume Manager server host

Model or Provider, where Model is the model name of the Virtual Enclosures and Provider is the name of the provider that manages the Virtual Enclosures

Configuration:

```
[Array:arrayAddress]
login= arrayUser
password=arrayPassword
model=cisco_mds
```

[EXP.BRIDGE]

The Bridge explorer section specifies discovery of devices that connect SCSI devices to fibre channel. (To some vendors, bridges are known as routers and gateways.)

For more information, see the administrator or user guide for your product.

`Disable=1 | 0`

1 = ON; 0 = OFF (default).

Disables/enables the Bridge explorer. The Bridge explorer is enabled by default.

`SNMPNameList=` *`bridgeAddress`*`[;`*`bridgeAddress`*`][;...]`

Place the bridge names or IP addresses of bridges to be explored in `SNMPNameList`. *`bridgeAddress`* can be either a bridge name, IP address, or a fully qualified domain name. For example:

`SNMPNameList=Bridge1;Router2;10.150.88.23`

You can specify more than one *`bridgeAddress`* by delimiting each with a semi-colon (;). The number of bridges is limited by the line length supported by `sal.conf` (10,000 characters).

The names in `SNMPNameList` and `Exp.Bridge:`*`bridgeAddress`* must match.

If the bridge is unavailable, exploration of the bridge fails and an error is logged to `syslog`.

`NodeNameList=` *`pathname`*`[;`*`pathname`*`][;...]`

For Solaris:

Provide the pathnames for bridges that SAL discovers in-band via a device node (OS handle). For example:

`NodeNameList = /dev/mynode;/home/someone/node`

You can specify more than one *`pathname`* by delimiting each with a semi-colon (;). The number of pathnames is limited by the line length supported by `sal.conf` (10,000 characters).

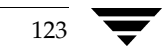
By default on Solaris, the Bridge explorer searches `/dev/scsi/processor/*` for device nodes.

For Windows:

The explorer searchs the Registry for Scsi adapters (includes FC HBAs that can be treated as SCSI HBAs). It then asks the HBA directly for details of its devices.

Enabling `DisableNodesearch` (setting `DisableNodeSearch = 1`) disables this feature.

The OS handle may also be explicitly listed here in a variable called: `NodeNameList`



If the device is claimed by a class driver then use its class handle (for example: Controller0:).

If it is unclaimed then it may be accessed via the SCSI port driver and the bus:target:lun information. For example:

`Scsi3:[0][2][1]` specifies controller 3, bus 0, target Id 2, lun 0

`NodeNameList=\\.\Controller0;\\.\scsi2[0][3][1]`

`DisableNodeSearch = 1 | 0`

0 = OFF (default); 1 = ON.

Disables/enables the Bridge explorer performing a `NodeNameList` search.
If on (Disable`NodeSearch = 1`), the explorer does not search the `/dev/scsi/processor` directory on Solaris, or search the Registry on Windows. It still attempts to process nodes listed in the `NodeNameList`.

`PublicCommunityName =` ***communityString***

By default, the SNMP community name that the Bridge explorer uses is `public`. If `PublicCommunityName` is present in the `[Exp.Bridge]` section, the Bridge explorer uses `PublicCommunityName` as the new SNMP community name for all bridges it explores.

You can override this community name for individual bridges with the following syntax:

`[Exp.Bridge:` ***bridgeAddress***`]`

`PublicCommunityName =` ***communityString***

bridgeAddress must be *identical* to a bridge address specified in `SNMPNameList`.

`iSCSIConnPort = n`

Specifies the port to use to discover FC-iSCSI routers. The default port is 5003.

If the FC-iSCSI router uses a different port, then you can specify separately for each router:

`[Exp.Bridge:routerInterfaceManagementHost]`

`iSCSIConnPort = n`

`routerInterfaceManagementHost` is the host assigned to the router's management interface, and can be a host name, qualified domain host name, or host IP address.

`routerInterfaceManagementHost` must be *identical* to its entry specified in `SNMPNameList`.

For example, if the listening iSCSI port is port 3260, then you would enter a new bridge section followed by a colon (:), the name of the host assigned to the router's management interface, and your iSCSI port number. Your entry would be similar to the following:

```
[Exp.Bridge:my_router_host]
iSCSIConnPort = 3260
```

[EXP.VHUB]

The Virtual Hub explorer section discovers switches running a hub emulation on one or more ports. These are known to SAL as virtual hubs, and include Brocade Communications QuickLoops.

SAL looks up switch names in its data store; however, for those switches requiring an administrative login, you must create a switch credentials entry. See "[Switch: switchName [;...]]" on page 126.

For more information, see the administrator or user guide for your product.

`Disable=1 | 0`

1 = ON; 0 = OFF (default).

Disables/enables the Virtual Hub explorer. The Virtual Hub explorer is enabled by default.

[EXP.EXCH]

This section configures exploration for VERITAS Storage Foundation for Microsoft Exchange Server.

For more information, see the administrator or user guide for your product.

`Disable=1 | 0`

0 = OFF (default); 1 = ON.

Disables/enables the Storage Foundation for Microsoft Exchange Server explorer. The explorer is enabled by default.

[CONFIGSAFE]

Enables saving a Brocade Communications switch configuration to a file and then restoring that configuration at a later time. Supports Brocade switches running with firmware 2.6 or above.

`Path = `*`pathname`*

Specifies the path to a file that contains Brocade switch configuration information. By default, SAL writes the Brocade switch configuration file to `/opt/VRTSspcs/sal/configSafe` (UNIX) and `\Program Files\Veritas\SANPoint Control\configSafe` (Microsoft Windows).

[SWITCH: *SWITCHNAME* [;...]]

Switch credentials sections are only used for those Brocade Communications switches requiring an administrative login.

For more information, see the administrator guide for your product.

Switch credentials are managed through `sal.conf`, but the passwords are automatically migrated to `switch.conf` at startup. The GS-3 Management Server Explorer (MGEX) first attempts to get credentials from `sal.conf`. MGEX then attempts to look up the credentials from the SAL data store.

SAL migrates switch credentials from `sal.conf` to `switch.conf` at startup, following a fabric exploration, and when switch credentials are configured via the XML API (such as with the SAL command line interface `vxsalcmd`). SAL replaces passwords in `sal.conf` with asterisks (*) when SAL migrates them to `switch.conf`. Modifying a switch credentials section in `sal.conf` will be reflected in `switch.conf` following a restart and in the store following a restart and a fabric traversal. Removing a switch credentials section will be reflected in `switch.conf` following a restart.

Note If `sal.conf` is updated via the XML API, no restart is necessary to activate changes. If `sal.conf` is updated manually, a restart is necessary.

For out-of-band MGEX exploration, the *switchName* must be the corresponding `SwitchNameList` entry. For in-band exploration and out-of-band SNMP exploration, the *switchName* must be the switch name, the switch World Wide Name (WWN), or switch IP address.

You can specify more than one *switchName* by delimiting each with a semi-colon (;). The number of switches is limited by the line length supported by `sal.conf` (10,000 characters).

If the switch is unavailable, exploration of the switch fails and an error is logged to `syslog`.

`Login =` *switchUser*
: Provide a valid username (*switchUser*) for switches requiring an administrative login for a SAL explorer to log on to the switch.

`Password =` *switchPassword*
: Provide a valid password (*switchPassword*) for switches requiring an administrative login for a SAL explorer to log on to the switch.

`Shared = 1 | 0`
: 0 = OFF (default); 1 = ON.

  When `Shared` is on (`Shared=1`) the switch credentials are shared by all switches in the fabric that contains the referenced switch. The default is off (`Shared=0`). This entry is used by the fabric traversal code and not by

MGEX out-of-band exploration. If set to 1, then the switch credentials will be migrated to all switch objects in the same fabric as the referenced switch (unless they have their own switch credentials section).

[EXP.VCS]

This section configures VERITAS Cluster Server exploration.

For more information, see the administrator guide for your product.

`Disable=1 | 0`

0 = OFF (default); 1 = ON.

Disables/enables explorer. The VERITAS Cluster Server explorer is enabled by default.

[EXP.TAPE]

This section configures tape enclosure exploration (UNIX only). The Tape explorer discovers tape enclosures from the information provided by the VERITAS NetBackup and HBA explorers.

For more information, see the administrator guide for your product.

`Disable=1 | 0`

0 = OFF (default); 1 = ON.

Disables/enables explorer. The Tape explorer is enabled by default.

[EXP.NBU]

This section configures the VERITAS NetBackup explorer (UNIX only). The NetBackup explorer runs on both the primary SAL and the remote SAL and discovers tape drive enclosures (tape drive serial numbers).

SAL contacts the tape robot using the NetBackup `libdevscan` API and discovers a list of its tape drive serial numbers. The tape drive serial numbers are stored on the tape robot `addrUnit`.

For more information, see the administrator guide for your product.

`Disable=1 | 0`

0 = OFF (default); 1 = ON

Disables/enables explorer. The VERITAS NetBackup explorer is enabled by default.

`LibDevScanDisable=1 | 0`

0 = OFF (default); 1 = ON

Disables/enables NBU Libdevscan inquiry. This inquiry sends SCSI commands to all tape robots and tape drives.

`LibDevScanDisable` is off by default.

[EXP.NBUAPP]

Configures the VERITAS NetBackup Application explorer. The NetBackup Application explorer discovers the host NetBackup application type. The explorer also accesses the NetBackup local database to discover NetBackup names for hosts and Shared Storage Option (SSO) information for tape robots and tape drives. Runs on primary and remote SALs on UNIX and Microsoft Windows.

`NBUSSODisable=1 | 0`

0 = OFF (default); 1 = ON

Disables/enables NBU Name and SSO discovery. This inquiry accesses NetBackup local database.

`NBUSSODisable` is off by default.

`Disable=1 | 0`

0 = OFF (default); 1 = ON

Disables/enables explorer. The VERITAS NetBackup explorer is enabled by default.

[EXP.CISCOMDS]

Configures the Cisco MDS explorer for exploration and management of Cisco MDS 9000 Family switches. Configure all Cisco switches with the same set of SNMP v1, v2c, or v3 credentials.

For more information, see the administrator guide for your product.

`Disable=1 | 0`

0 = OFF (default); 1 = ON

Disables/enables the Cisco MDS switch explorer. The explorer is enabled by default. If a value is not specified for `Disable`, or there is no `Disable` variable, the explorer is enabled. If you are exploring Cisco MDS switches with the Cisco MDS explorer, ensure that Cisco switch exploration by the MGEX explorer is disabled to avoid conflicts. If there are Cisco switches that the Cisco MDS explorer cannot access, enable the MGEX explorer for Cisco switch exploration. For more information, see "[MGEX]" on page 107.

`SwitchNameList=`*switchAddress*`[;`*switchAddress*`][;...]`

switchAddress can be either a switchname, IP address, or a fully qualified domain name. *switchAddress* specifies the Cisco MDS switch address to communicate with the switch using SNMP protocol.

You can specify more than one *switchAddress* by delimiting each with a semi-colon (;). The number of switches is limited by the line length supported by `sal.conf` (10,000 characters).

If the switch is unavailable, exploration of the switch fails and an error is logged to `syslog`.

`SNMPVersion=1 | 2c | 3`

Specifies the SNMP version used by the SNMP agent on the Cisco MDS 9000 series switches. Cisco recommends using version 3 for increased security. SAL requires that the SNMP credentials for the switches be network-admin or another role with read/write permissions.

`SNMPCommunityName=`*`communityString`*

SNMP community name that the Cisco MDS explorer uses for all Cisco MDS switches that it explores. Valid for SNMP versions 1 and 2c. All Cisco switches using v1 or v2c must have the same community name. The default value in the Cisco MDS 9000 series switches is null.

`SNMPSecurityLevel= noAuthNoPriv | authNoPriv | authPriv`

Security level expected by the SNMP agents running on the Cisco MDS switches. Valid for SNMP version 3 only.

`noAuthNoPriv` = no authentication and no privacy

`authNoPriv` = with authentication and no privacy

`authPriv` = with authentication and privacy

`SNMPAuthProtocol= MD5 | SHA`

Authentication protocol used by the SNMP agents running on the Cisco MDS switches. Valid for SNMP version 3 only. The default value in the Cisco MDS 9000 series switches is `MD5`.

`SNMPUserName=`*`userNameString`*

Identifies the username to log on to the Cisco MDS switches. Required if authentication is enforced by the SNMP agents. Valid for SNMP version 3 only.

`SNMPAuthPassPhrase=passPhraseString`

Identifies the authentication password phrase to log on to the Cisco MDS switches. Required if authentication is enforced by the SNMP agents. Valid for SNMP version 3 only. When SAL first reads the password from `sal.conf`, SAL encrypts the password, places the password in another file, and replaces the password in `sal.conf` with asterisks (*).

`SNMPPrivProtocol=D | E | S`

Identifies the privacy protocol used by the SNMP agents running on the Cisco MDS switches. Required if privacy is enforced by the SNMP agents. Valid for SNMP version 3 only.

`SNMPPrivPassPhrase=`*`privPassPhraseString`*

Identifies the privacy password phrase to log on to the Cisco MDS switches. Required if privacy is enforced by the SNMP agents. Valid for SNMP version 3 only. When SAL first reads the password from `sal.conf`, SAL encrypts the password, places the password in another file, and replaces the password in `sal.conf` with asterisks (*).

NOTES

It is not possible to reconfigure the port that SAL remotes use; SAL remotes always use port 2802.

On the QuickStart Server, `sal.conf` resides in `/var/VRTSspcq`

On the QuickStart Agent, `sal.conf` resides in `/opt/VRTSsal`

SANPoint Control QuickStart creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to access the SANPoint Control QuickStart scripts and commands.

Note On Solaris, you normally find two files listed. The file in `/opt/VRTSspcs/sal/sal.conf` is a symbolic link to the actual file located in `/var/VRTSspcs/sal.conf` (or in the user-specified directory during installation). (Of course editing `/opt/VRTSspcs/sal/sal.conf` will also reflect changes in the actual file.)

Maximum line length in `sal.conf` is 10,000 characters.

SEE ALSO

"spcconfig" on page 93

"vxDB2" on page 98

"vxOra" on page 100

"vxsal" on page 131

vxsal

NAME

vxsal - startup/shutdown script for SAL

SYNOPSIS

```
vxsal start | stop | restart | status | version
```

DESCRIPTION

`vxsal` is the (UNIX-only) startup/shutdown script for the SAN Access Layer (SAL) daemon—`vxsald`.

OPTIONS

`start`
: Invokes the SAL daemon/service (`vxsald`).

`stop`
: Stops `vxsald`.

`restart`
: Stops `vxsald` and then invokes `vxsald`.

`status`
: Displays HBA and device driver information without starting or stopping `vxsald`. You can run `vxsal` with the `status` option on a remote SAL at anytime—`vxsald` can be running or stopped when you invoke `vxsal status`.

`version`
: Displays `vxsald` version and copyright information.

NOTES

On the QuickStart Server and Agent, `vxsal` resides in `/opt/VRTSsal`

SANPoint Control QuickStart creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to access the SANPoint Control QuickStart scripts and commands.

On QuickStart Agents, `vxsal` initiates and terminates a remote SAL (`vxsald`).

SEE ALSO

"spcconfig" on page 93

"sal.conf" on page 102

"vxsald" on page 133

vxsald

NAME

vxsald - initiates SAL

SYNOPSIS

```
vxsald [-initdb | -version ]
```

DESCRIPTION

`vxsald` initiates the SAL (SAN Access Layer) daemon.

OPTIONS

`-version`

Display version information. The daemon does not terminate after displaying the version info.

NOTES

On the QuickStart Server and Agent, `vxsald` resides in `/opt/VRTSsal`

SANPoint Control QuickStart creates symbolic links to all its scripts and commands in the `/opt/VRTS/bin` directory at installation. Add `/opt/VRTS/bin` to your host's `PATH` environment variable to access the SANPoint Control QuickStart scripts and commands.

On UNIX, you normally use `vxsal` to start and stop the remote SAL(s). See "vxsal" on page 131 for more information.

The primary SAL is a centralized server in a SAN, and is in charge of the following tasks:

- Controlling remote daemons
- Maintaining database
- Communicating with clients including GUI and Web browser

Remote SALs collect information such as local host, LDDL, and HBA (host bus adapter) data and send it to the primary SAL.

SEE ALSO

"spcconfig" on page 93

"sal.conf" on page 102

"vxsal" on page 131

Troubleshooting B

This section explains how to handle issues related to installing, configuring, and operating SANPoint Control QuickStart. It also provides help for solving problems related to system performance.

This section contains the following topics:

"Installation Issues" on page 136

"Configuration Issues" on page 137

"Oracle Discovery Issues" on page 140

"VERITAS NetBackup Discovery Issues" on page 141

"VERITAS Volume Manager Discovery Issues" on page 142

"VERITAS Cluster Server Discovery Issues" on page 143

"Performance Issues" on page 144

"Issues When Starting and Stopping SANPoint Control QuickStart Components" on page 145

"Connection Issues" on page 146

Installation Issues

This section explains how to fix installation problems such not being able to run the installation programs.

Installation Issues

Problem	Explanation	Solution
Can't run install script	You may not be logged in as root.	Log in as a user who does have the appropriate rights.
	The system may not have enough disk space.	Check the system log. Check the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*. If necessary, make more disk space available. See your vendor documentation.

Configuration Issues

This section explains how to fix problems such as devices not showing up in the `spcconfig` report.

Configuration Issues

Problem	Explanation	Solution
Upon startup, the HBA explorer complains that the common HBA library is not installed properly: /etc/hba.conf does not exist	Fabric discovery on a system with a Tachyon driver requires common HBA support.	SANPoint Control QuickStart Server or SANPoint Control QuickStart Agent hosts using HBAs with the Tachyon driver must have the Common HBA Library installed. If the Common HBA Library is not available, SANPoint Control QuickStart regards the HBA as being offline and does not explore the fabric through that HBA.
The `spcconfig` report wasn't written to the disk	You may not have enough room on the disk.	Choose another destination or make space available, if necessary. See your vendor documentation
	You may not have the rights to write to the disk.	Log in as a user with read-write rights and try again.
Device didn't show up in the `spcconfig` report	The device may not be supported.	Check the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* to make sure the device is supported. (Note that, if the device is not supported, SANPoint Control QuickStart can still discover it as a generic device. Then, you can enclose it and add attributes.
	If the device is supported, SNMP may not be enabled on that device.	Enable SNMP on that device. See your vendor documentation.

Configuration Issues

Problem	Explanation	Solution
	The SNMP agent on the device may be overloaded.	Check the CPU utilization on the device. Troubleshoot as needed. See your vendor documentation.
	Network delays may be causing SNMP requests to time out.	Check the network route from the host to the device. Troubleshoot as needed. See your vendor documentation.
	The subnet specified for `spcconfig` may not be correct.	Make sure the subnet you used when running `spcconfig` was correct. If necessary, rerun `spcconfig` with the correct subnet. Check with your network administrator.
	The device may be on a private network.	Provide access to the device, if needed. See your vendor documentation.
	You may be using the wrong version of `spcconfig`.	Run `spcconfig -v` to make sure you are using the same version as SANPoint Control QuickStart.
HBA didn't show up in the `spcconfig` report	The HBA, its firmware, or its driver may not be supported.	Check the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*.
	There may be a problem with the HBA that is preventing the driver from loading.	Use the HBA vendor diagnostics to make sure the HBA is functioning properly. See the vendor documentation.
Updatesto server configuration didn't take effect	You may not have the appropriate rights or permissions.	Make sure you are running `spcconfig` as root on Solaris.
	`vxsald` may not have restarted.	Stop and restart `vxsald`.

Configuration Issues

Problem	Explanation	Solution
	If you reinstalled SANPoint Control QuickStart, it may not have your old settings.	Run `spcconfig` to update the configuration file automatically.
Two `sal.conf` files were installed	One of the instances is actually a link to the file.	Refer to "sal.conf" on page 102.
	The install script creates the `sal.conf` file as well as a link to the file. The link may have been broken, which would result in two separate `sal.conf` files.	Recreate the softlink.
Can't add switches manually for MGEX Explorer to discover out-of-band	The explorer may be set to verify vendor IDs within WWNs. However, because the list of vendor IDs in SANPoint Control QuickStart are based on the IEEE vendor table, which can be updated with new vendor IDs at any time, new vendor IDs may not be in the list.	Disable Verify Vendor ID within WWNs. Set `VerifyVendor = 0` Refer to "sal.conf" on page 102.
`spcconfig` disabled the HBA Explorer	If a host has more than one HBA and at least one of them is unsupported, `spcconfig` disables the HBA Explorer.	Check the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List* to make sure all of the HBAs are supported.
Can't create or write to the SANPoint Control QuickStart store	The system may not have enough disk space.	If the system log indicates that that is the problem, check the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*. If necessary, make more disk space available. See your vendor documentation

Oracle Discovery Issues

This section explains how to fix problems such as not being able to discover Oracle instances.

Oracle Discovery Issues

Problem	Explanation	Solution
Can't discover Oracle instances	The Oracle Explorer may be disabled.	Enable the explorer if necessary. See *SANPoint Control Administrator's Guide*.
	Oracle may not be running.	Make sure Oracle is running. See your vendor documentation.
	Oracle version may be unsupported.	Check the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*.
	The Oracle Explorer may have been run by a user without DBA privileges.	Restart the explorer. When prompted, specify a user that has DBA privileges. Refer to "vxOra" on page 100.
Can't add, edit, or delete Oracle instances from theOracle discovery configuration file	The configuration file, `vxOra.conf`, may be missing or corrupted.	Restore a backup copy of the file, or create a new one by running `vxOra` again. Refer to "vxOra" on page 100.
Can't run the Oracle Explorer	You may not be logged in as root on UNIX.	Make sure you are logged in with the appropriate rights. Try restarting the explorer. Refer to "vxOra" on page 100.

VERITAS NetBackup Discovery Issues

This section explains how to fix problems such as not being able to find NetBackup.

VERITAS NetBackup Discovery Issues

Problem	Explanation	Solution
Can't discover NetBackup instances	NetBackup may not be running.	Make sure NetBackup is running. See the NetBackup documentation.
	NetBackup version may be unsupported.	Check the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*.
Can't discover NetBackup Client; however SANPoint Control QuickStart discovers and properly visualizes the NBU Master Server/Media Server.	The SANPoint Control NBU explorer aborts the discovery, when neither the SANPoint Control QuickStart Agent host nor the NBU Master Server host names are qualified.	Make sure that both the SANPoint Control QuickStart host and the NBU Master Server host names are configured to register their domain suffix with Domain Name Service (DNS).
The NBUName attribute on a tape drive keeps changing from one name to another	If two hosts have access to the same tape drive, the hosts may assign two different NetBackup names to the same drive. This setup is not correct.	Assign the same name to the drive. See the NetBackup documentation.
The SSO attribute on a tape drive keeps changing from one name to another	If two hosts have access to the same tape drive, the drive may not be set up as an SSO tape drive.	Set up the drive as an SSO drive. See the NetBackup documentation.

VERITAS Volume Manager Discovery Issues

This section explains how to fix problems such as not being able to find VERITAS Volume Manager.

VERITAS Volume Manager Discovery Issues

Problem	Explanation	Solution
Can't discover discover Volume Manager instances	The Volume Manager Explorer may be disabled.	Enable the explorer if necessary. Refer to "sal.conf" on page 102.
	Volume Manager may not be running.	Make sure Volume Manager is running.
	Volume Manager version may be unsupported.	Check the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*.

VERITAS Cluster Server Discovery Issues

This section explains how to fix problems such as not being able to find VERITAS Cluster Server instances.

VERITAS Cluster Server Discovery Issues

Problem	Explanation	Solution
Can't discover Cluster Server instances	The Cluster Server Explorer may be disabled.	Enable the explorer if necessary. Refer to "sal.conf" on page 102.
	Cluster Server may not be running.	Make sure Cluster Server is running.
	Cluster Server version may be unsupported.	Check the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*.
Cluster is discovered, but no service groups and resources	Cluster service may not be in the RUNNING state.	Run `hasys -state` to make sure the states of the systems in the cluster are healthy. See the Cluster Server documentation.
	There may not be any service groups or resources configured on the cluster.	See the Cluster Server documentation.
Storage used by the service groups are not highlighted in the GUI	The Cluster Server resources that use the storage may not be configured correctly.	See the Cluster Server documentation.

Performance Issues

This section explains how to fix problems such as slow performance, increases in logged data, and so on.

Performance Issues

Problem	Explanation	Solution
The CPU utilization on the SANPoint Control Server is high	The network may be experiencing performance problems.	Test network performance and troubleshoot as necessary. See your vendor documentation.
	The CPU may not meet the system requirements.	Check the system requirements in the *VERITAS SANPoint Control QuickStart 4.0 Hardware and Software Compatibility List*. Upgrade if necessary.
The Console hangs	The host may have run out of disk space.	Check the system log. If necessary, make more disk space available. See your vendor documentation

Issues When Starting and Stopping SANPoint Control QuickStart Components

This section explains how to fix problems such as not being able to run commands from the command line, getting port errors when trying to start SANPoint Control QuickStart, and so on.

Issues When Starting and Stopping SANPoint Control QuickStart Components

Problem	Explanation	Solution
Can't run commands from the command line	You may not be logged in as root on UNIX.	Make sure you are logged in with the appropriate rights. Try rerunning the command.
Get a port error when trying to start SANPoint Control QuickStart	The ports used by SANPoint Control QuickStart may not have been released yet.	Try pinging the host to see if it responds. After stopping SANPoint Control QuickStart processes or daemons, wait about thirty seconds before starting them again. This gives the operating system time to free up logical ports and other resources that the SANPoint Control QuickStart processes need upon restart. See "vxsal" on page 131.
	You may have the wrong port number or the port number may have been changed.	Check the port number being used. See "Firewall Requirements" on page 27.

Connection Issues

This section explains how to fix problems such as not being able to connect to the QuickStart Server.

Connection Issues

Problem	Explanation	Solution
Can't connect to QuickStart Server from VEA Console	`vxsald` may not be installed or running on that host.	Check to see if `vxsald` is running. See "vxsal" on page 131.
	The login information may not be correct.	Make sure the login information is correct and that there are no typographical errors.
	The hostname may not be resolving to the IP address correctly.	Try using the IP address of the SANPoint Control QuickStart Server.
	The hostname or IP address specified in the VEA Console may be incorrect.	Check to make sure the SANPoint Control QuickStart Server hostname or IP address is correct and doesn't contain any typographical errors.
	The VEA Console may not have network access to the QuickStart Server.	Check network connections to make sure the QuickStart Server and VEA Console have access to each other. See your vendor documentation.

SANPoint Control QuickStart and Dependency Installation Packages C

This section lists the SANPoint Control QuickStart installation packages and the additional packages on which QuickStart is dependent. Packages are grouped by base packages and language-related packages.

Note For more information about locating packages and installing language-related packages, consult the *Storage Solutions Installation Guide*.

The following table lists the SANPoint Control QuickStart base packages:

SANPoint Control QuickStart and Its Dependent Base Packages

Description	Package Name
SANPoint Control QuickStart Server package	VRTSspqs
SANPoint Control QuickStart Documentation package	VRTSspqdc
SANPoint Control QuickStart Manual Pages package	VRTSspqmn
SANPoint Control QuickStart Configuration Utility package	VRTSspcfg
VERITAS SAN Access Layer (SAL) package	VRTSsal
VERITAS vLicense package	VRTSvlic
VERITAS Enterprise Administrator Server package	VRTSob
VERITAS Enterprise Administrator Client package	VRTSobgui
VERITAS PERL package	VRTSperl

The following table lists the base SANPoint Control QuickStart language-related packages:

SANPoint Control QuickStart Language-Related Packages

Description	Package Name
VERITAS SANPoint Control QuickStart Japanese package	VRTSjasmq
VERITAS SANPoint Control QuickStart Documentation Japanese package	VRTSjasmd
VERITAS SANPoint Control QuickStart Manual Pages Japanese package	VRTSjasmn
VERITAS Enterprise Administrator Server Multi-Language package	VRTSmuob
VERITAS Enterprise Administrator Console Multi-Language package (Solaris)	VRTSmuobg
VERITAS Enterprise Administrator Console Multi-Language package (Windows)	VRTSmuobg.msi
VERITAS vLicense Multi-Language package	VRTSmulic

Index

A

application interoperability
- IBM DB2 EE and EEE 13
- Oracle 14
- VERITAS Cluster Server 12
- VERITAS NetBackup 11
- VERITAS Volume Manager 10

B

Bridge explorer
- adding bridges 74
- adding routers 74
- removing bridges 81
- removing routers 81

bridge interoperability
- Chaparral 38
- Crossroads 39
- Hewlett-Packard 40

bridges
- adding 74
- exploring 74
- removing from discovery 81

Brocade
- credentials 72
- QuickLoops 125
- switch interoperability 16
- zone aliases 17

C

Chaparral
- bridge interoperability 38

Cisco
- router interoperability 37
- switch interoperability 19

Cisco MDS
- discovery parameters
  - modifying switches 68

Cisco MDS explorer
- discovery parameters
  - adding switches 68
- SNMP v3 68

CLIs
- running commands
  - troubleshooting 145

configuration
- multi-fabric 3
- single-fabric 3
- typical 3

configuration files
- `sal.conf` 102

configuration. *See* interoperability

configuring
- device discovery 61
- port 2148 for host 27
- port 2802 for host 27
- SPC Server 93

connecting
- QuickStart Server 85

contacting VERITAS xxi

CPU utilization 144

credentials
- Brocade QuickLoops 72
- Brocade switches 72
- switches 72

Crossroads
- bridge interoperability 39

CT Passthru
- disabling 77

D

daemons
- QuickStart Agent 84
- QuickStart Server 84
- `vxsald` 133

DAS
HBA explorer disabled 65
OS Handles pane 65
VERITAS File System discovery 65
VERITAS Volume Manager
discovery 65
data store
troubleshooting 139
DB2
interoperability 13
SANPoint Control QuickStart
explorer 98
default user accounts 85
dependency packages. *See* packages
devices
discovery 61
inventorying 93
removing, discovery for 78
direct attached storage. *See* DAS
discovery 61
Bridge explorer 74, 81
Cisco MDS explorer 68
disabling CT Passthru 77
HBAs
troubleshooting 138, 139
maximizing 5
MGEX Explorer
troubleshooting 139
Oracle
troubleshooting 140
overview 63
quickloops 125
removing SAN devices 78
SAN devices, removing 78
SANPoint Control QuickStart Agents 66
SNMP explorer 79
VERITAS Cluster Server
troubleshooting 143
VERITAS Volume Manager
troubleshooting 142
discovery. *See* interoperability
disks
IDE DAS 65
SCSI DAS 65

E

Emulex
HBA interoperability 30
miniport driver 31
enabling
out-of-band communication 53
QuickStart Agent switch exploration 67
explorers
Bridge 74, 81
Cisco MDS 68
DB2 98
MGEX
CT Passthru 77
in-band 17, 21, 23
out-of-band 17
Oracle 75
SNMP 79

F

fabrics
remote 66
firewall
configuring
port 2148 27
port 2802 27

H

HBA explorer
disabled 65
HBA interoperability
Emulex 30
JNI 32
QLogic 34
HBAs
discovery 66
troubleshooting 138, 139
unsupported 57
Hewlett-Packard
bridge interoperability 40
host
port 2148 27
port 2802 27
host_dd_mm_yyyy_hh_mm_ss.csv 57
host_dd_mm_yyyy_hh_mm_ss.html 57

I

IBM DB2
interoperability 13
IDE disks
DAS 65
initiating
`sald` 131
INRANGE
switch interoperability 21

install
UNIX
troubleshooting 136
installation
multi-language packages 147
packages 147
installing
QuickStart
multi-fabric SANs 3
single-fabric SAN 3
QuickStart Agent 44
QuickStart Server 42
VEA Console
Solaris 46
Windows 46
interoperability
Brocade switches 16
Chaparral bridges 38
Cisco routers 37
Cisco switches 19
Crossroads bridges 39
Emulex HBAs 30
Hewlett-Packard bridges 40
IBM DB2 13
INRANGE switches 21
JNI HBAs 32
McDATA switches 23
Oracle 14
QLogic HBAs 34
QLogic switches 25
VERITAS Cluster Server 12
VERITAS NetBackup 11
VERITAS Volume Manager 10
inventorying your SAN 93

J

JNI
HBA configuration file 32
HBA interoperability 32
JNI EZ Fibre configuration utility 33

L

logging
troubleshooting 144
logging in
QuickStart Server 85
login credentials 85
QuickLoops, Brocade 72
switches, Brocade 72
virtual hubs 72

M

McDATA
switch interoperability 23
MGEX Explorer
out-of-band discovery
troubleshooting 139
MGEX explorer
CT Passthru 77
multi-fabric SANs 3, 66
multi-language packages
list 147

O

Oracle
discovery
troubleshooting 140
interoperability 14
Oracle explorer 75
configuration 75
OS Handles pane
DAS 65
out-of-band communication
enabling 53

P

packages
dependencies 147
installation 147
list 147
permissions
QuickStart user accounts 85
physical connections. *See* interoperability
polling
troubleshooting 144
ports
2148, host 27
2802, host 27
errors at startup
troubleshooting 145

Q

QLogic
HBA interoperability 34
switch interoperability 25
quickloops 125

R

remote fabrics 66
reports
SANPoint Control QuickStart
Configuration Utility 51

restarting
vxsald
troubleshooting 138
restarting SANPoint Control QuickStart Server 84
root user 42
router interoperability
Cisco 37
routers
adding 74
exploring 74
removing from discovery 81
running
QuickStart Agent 84
SANPoint Control QuickStart Configuration Utility 53
VEA Console
Solaris 85
Windows 85

S

SAL. *See* SANPoint Control Server
sal.conf
configuring 102
MGEX
CT Passthru 77
sal.conf
creating 51
troubleshooting 139
updating 51
sald 102, 133
configuring 102
SAN Access Layer
daemon 133
SAN discovery configuration file. *See* sal.conf
SAN discovery data store
size factors 5
SANPoint Control QuickStart
discovery configuration 61
multi-fabric configuration 3
single-fabric configuration 3
typical configuration 3
user account privileges 85
SANPoint Control QuickStart Agent
disabling CT passthru 77
discovery 66
discovery role 5
host choice 5
install location 5
installing 44
relationship to SANPoint Control QuickStart Server 5
removing 78
restarting 84
running 84
starting 84
startup and shutdown script 84
stopping 84
switch exploration 67
uninstalling
Solaris 88
SANPoint Control QuickStart Configuration Utility
overview 51
reports 51
running 53
SANPoint Control QuickStart Server
configuration files 102
configuring
Agent discovery 66
connecting 85
disabling CT passthru 77
host and switch zoning 5
host choice 5
install location 5
installing 42
login credentials 85
principal switch connection 5
restarting 84
starting 84
startup and shutdown script 84
stopping 84
uninstalling 88
SANPoint Control Server
connection from Console
troubleshooting 146
scripts
vxsal 84, 131
SCSI disks
DAS 65
Server database
troubleshooting 144
service groups
troubleshooting 143
shutting down
sald 131
single-fabric SAN 3

SNMP
agent
troubleshooting 137
providing access
troubleshooting 137
SNMP discovery parameters
removing switches 79
SNMP v3
authentication privacy credentials 68
Solaris
installing
QuickStart Agent 44
QuickStart Server 42
VEA Console 46
running
VEA Console 85
running QuickStart Agent 84
uninstalling
QuickStart Agent 88
QuickStart Server 88
VEA Console 90
user rights 42
`spcconfig` 93
troubleshooting 137, 138
`spcconfig` report
viewing 57
`spcconfig` reports 51
hyperlinked IP addresses 57
`spcconfig`. *See* SANPoint Control QuickStart Configuration Utility
startup
port errors
troubleshooting 145
stopping
`vxsald`
troubleshooting 138
switch credentials
adding 72
switch exploration
QuickStart Agents 67
switch interoperability
Brocade 16
Cisco 19
INRANGE 21
McDATA 23
QLogic 25
switches
Cisco MDS explorer
adding 68
modifying 68
MGEX
in-band 17, 21, 23
out-of-band 17
SNMP explorer
removing 79

T

terminating
`sald` 131
troubleshooting 144
contacting VERITAS xxi
using VRTSexplorer xxi

U

uninstalling
QuickStart Agent
Solaris 88
QuickStart Server
Solaris 88
VEA Console 90
Solaris 90
Windows 90
unsupported HBAs 57
updating
Server configuration
troubleshooting 138
user accounts
default 85
permissions 85

V

VEA Console
connection to Server
troubleshooting 146
troubleshooting 144
VERITAS Cluster Server
discovery
troubleshooting 143
interoperability 12
VERITAS Enterprise Administrator (VEA)
Console
Solaris installing 46
Solaris running 85
Solaris uninstalling 90
Windows installing 46
Windows running 85
Windows uninstalling 90

VERITAS Enterprise Administrator (VEA) Console
host choice 6
install location 6
VERITAS File System
DAS discovery 65
VERITAS NetBackup
interoperability 11
troubleshooting 141
VERITAS Volume Manager
DAS discovery 65
discovery
troubleshooting 142
interoperability 10
viewing `spcconfig` report 57
virtual hubs
credentials 72
VRTSexplorer
using to troubleshoot xxi
`VRTSob` 147
`VRTSobgui` 147
`VRTSperl` 147
`VRTSsal` 147
`VRTSspcfg` 147
`VRTSspqdc` 147
`VRTSspqmn` 147
`VRTSspqs` 147
`VRTSvlic` 147
`vxDB2` 98
`vxOra` 75, 100
`vxsal` 84, 131
`vxsald`
troubleshooting 138

W

Windows
installing
VEA Console 46
running
VEA Console 85
uninstalling
VEA Console 90

Z

zone aliases
Brocade switches 17