

NetApp® Host Agent 2.3

Installation Guide

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: <http://www.netapp.com>

Part number 215-01617_A0
February 2006

Copyright and trademark information

Copyright information

Copyright © 1994–2006 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Portions of this product are derived from the Berkeley Net2 release and the 4.4-Lite-2 release, which are copyrighted and publicly distributed by The Regents of the University of California.

Copyright © 1980–1995 The Regents of the University of California. All rights reserved.

Portions of this product are derived from NetBSD, which is copyrighted by Carnegie Mellon University.

Copyright © 1994, 1995 Carnegie Mellon University. All rights reserved. Author Chris G. Demetriou.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted, provided that both the copyright notice and its permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS “AS IS” CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Software derived from copyrighted material of The Regents of the University of California and Carnegie Mellon University is subject to the following license and disclaimer:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notices, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER

IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software contains materials from third parties licensed to Network Appliance Inc. which is sublicensed, and not sold, and title to such material is not passed to the end user. All rights reserved by the licensors. You shall not sublicense or permit timesharing, rental, facility management or service bureau usage of the Software.

Portions developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999 The Apache Software Foundation.

Portions Copyright © 1995–1998, Jean-loup Gailly and Mark Adler

Portions Copyright © 2001, Sitraka Inc.

Portions Copyright © 2001, iAnywhere Solutions

Portions Copyright © 2001, i-net software GmbH

Portions Copyright © 1995 University of Southern California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of Southern California, Information Sciences Institute. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

Portions of this product are derived from version 2.4.11 of the libxml2 library, which is copyrighted by the World Wide Web Consortium.

Network Appliance modified the libxml2 software on December 6, 2001, to enable it to compile cleanly on Windows, Solaris, and Linux. The changes have been sent to the maintainers of libxml2. The unmodified libxml2 software can be downloaded from <http://www.xmlsoft.org/>.

Copyright © 1994–2002 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>

Software derived from copyrighted material of the World Wide Web Consortium is subject to the following license and disclaimer:

Permission to use, copy, modify, and distribute this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications, that you make:

The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.

Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, a short notice of the following form (hypertext is preferred, text is permitted) should be used within the body of any redistributed or derivative code: "Copyright © [\$date-of-software] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>.

Notice of any changes or modifications to the W3C files, including the date changes were made.

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS

FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

Software derived from copyrighted material of Network Appliance, Inc. is subject to the following license and disclaimer:

Network Appliance reserves the right to change any products described herein at any time, and without notice. Network Appliance assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Network Appliance. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Network Appliance.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the Network Appliance logo, the bolt design, NetApp—the Network Appliance Company, DataFabric, Data ONTAP, FAServer, FilerView, MultiStore, NearStore, NetCache, SecureShare, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapVault, SyncMirror, and WAFL are registered trademarks of Network Appliance, Inc. in the United States, and/or other countries. gFiler, Network Appliance, SnapCopy, Snapshot, and The Evolution of Storage are trademarks of Network Appliance, Inc. in the United States and/or other countries and registered trademarks in some other countries. ApplianceWatch, BareMetal, Camera-to-Viewer, ComplianceClock, ComplianceJournal, ContentDirector, ContentFabric, EdgeFiler, FlexClone, FlexVol, FPolicy, HyperSAN, InfoFabric, LockVault, Manage ONTAP, NOW, NOW NetApp on the Web, ONTAPI, RAID-DP, RoboCache, RoboFiler, SecureAdmin, Serving Data by Design, SharedStorage, Simulate ONTAP, Smart SAN, SnapCache, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapMigrator, SnapSuite, SnapValidator, SohoFiler, vFiler, VFM, Virtual File Manager, VPolicy, and Web Filer are trademarks of Network Appliance, Inc. in the United States and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of Network Appliance, Inc. in the United States. Spinnaker Networks, the Spinnaker Networks logo, SpinAccess, SpinCluster, SpinFS, SpinHA, SpinMove, and SpinServer are registered trademarks of Spinnaker Networks, LLC in the United States and/or other countries. SpinAV, SpinManager, SpinMirror, SpinRestore, SpinShot, and SpinStor are trademarks of Spinnaker Networks, LLC in the United States and/or other countries.

Apple is a registered trademark and QuickTime is a trademark of Apple Computer, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

Network Appliance is a licensee of the CompactFlash and CF Logo trademarks.

Network Appliance NetCache is certified RealSystem compatible.

Table of Contents

	Preface	.ix
Chapter 1	Overview of NetApp Host Agent	1
	Before reading further	2
	How NetApp Host Agent works	3
Chapter 2	Using the NetApp Host Agent for SRM	5
	Prerequisites for SRM	6
	About SRM	8
	About NetApp Host Agent for SRM	10
Chapter 3	Using the NetApp Host Agent for SAN	13
	Assumptions	14
	How NetApp Host Agent functions in a SAN	16
Chapter 4	Installing NetApp Host Agent	19
Chapter 5	Using NetApp Host Agent.	21
	Starting and stopping the NetApp Host Agent service	22
	Accessing the user interface	23
	User privileges and security	24
	Configuring NetApp Host Agent	25
	The NetApp Host Agent log file	28

Preface

About this guide

This guide provides an overview of the NetApp® Host Agent 2.3 software product and describes how to set up and use NetApp Host Agent with DataFabric Manager to monitor and manage SAN or SRM hosts.

This guide does not cover basic system or network administration topics, such as IP addressing and network management; it emphasizes the characteristics of integrated management of NetApp appliances and related systems.

This guide describes the views, options, and operations available in the NetApp Host Agent web-based user interface.

Who this guide is for

This guide is written for system administrators and anyone interested in NetApp appliance management.

This guide assumes that you are familiar with the client-side operating systems UNIX® and Windows®.

Terminology conventions

When the term “appliance” is used, the information applies to all Network Appliance™ filers, NetCache® appliances, NearStore® systems, FAS appliances, and in some cases fibre channel switches.

When the term “filer” is used, it can mean any NetApp storage appliance — filer, FAS appliance, or NearStore system.

This guide uses the term “type” to mean pressing one or more keys on the keyboard. It uses the term “enter” to mean pressing one or more keys and then pressing the Enter key, such as when you enter a command at the command line.

Path convention

In parenthetical references to paths leading to parts of the DataFabric™ Manager user interface, the greater-than symbol (>) is used to point to the next interface element connecting you to your final destination. For example, File Systems > Views > Volume Growth means to select the File Systems tab, then open the Views drop-down list and select Volume Growth.

**Keyboard
conventions**

When describing key combinations, this guide uses the hyphen (-) to separate individual keys. For example, “Ctrl-D” means pressing the “Control” and “D” keys simultaneously. Also, this guide uses the term “Enter” to refer to the key that generates a new paragraph (a “carriage return”), although the key is named “Return” on some keyboards.

**Typographic
conventions**

The following table describes the typographic conventions used in this guide.

Convention	Type of information
<i>Italic type</i>	Words or characters that require special attention. Placeholders for information you must supply. For example, if the guide says to enter the <code>dfm alarm destroy alarm-ids</code> command, you enter the characters “dfm alarm destroy” followed by the id of the alarm you want to destroy. Book titles in cross-references.
Monospaced font	Command and daemon names. Information displayed on the system console or other computer monitors. The contents of files.
Bold monospaced font	Words or characters you type. What you type is always shown in lowercase letters, unless you must type it in uppercase letters.

About this section This chapter provides an overview of the NetApp Host Agent 2.1 software and describes its SAN and SRM capabilities.

Topics in this section This section contains information about the following topics:

- ◆ [“Before reading further”](#) on page 2
- ◆ [“How NetApp Host Agent works”](#) on page 3

Before reading further

Terms and technologies you should know

Before you read about how to use NetApp Host Agent, you must familiarize yourself with the following terms and technologies:

- ◆ NetApp Host Agent
- ◆ Host agent
- ◆ SAN host
- ◆ SRM
- ◆ SnapDrive™ software
- ◆ Microsoft Cluster Services (MSCS)

NetApp Host Agent: An independent software application that resides on a non-NetApp host that you want to monitor with DataFabric Manager.

Host agent: Any Windows, Solaris, or Linux host running the NetApp Host Agent software. If the host agent has SAN hardware, it can also be referred to as a SAN host.

SAN host: A SAN host is a Storage Area Network (SAN) device, such as a UNIX or Windows system, that sends requests to other SAN devices in a SAN to perform tasks. To be monitored by DataFabric Manager, a SAN Host must be running the NetApp Host Agent software.

SRM: Storage Resource Management. SRM is the monitoring and management capability of storage resources, including applications, files, file systems, and networks. This document uses the term SRM to refer specifically to file-level and directory-centric SRM data.

SnapDrive: The NetApp SnapDrive software, which configures space on NetApp storage systems as local disks on Windows hosts, is required for LUN management when NetApp Host Agent is providing the SAN Host functionality on a Windows platform.

Microsoft Cluster Services (MSCS): The Microsoft Cluster Services (MSCS) is a clustering technology for Windows servers. If one of the clustered servers fails, the other server in the cluster takes over for the failed server, providing fault tolerance and increasing server availability.

How NetApp Host Agent works

About the NetApp Host Agent

NetApp Host Agent is an independent software application that resides on a non-NetApp host that you want to monitor with DataFabric Manager. NetApp Host Agent enables remote DataFabric Manager management stations to access those hosts in a secure and platform independent way.

To enable DataFabric Manager discovery of hosts, the NetApp Host Agent software must be installed on each host that you want to monitor and manage. After you install the NetApp Host Agent software, the host will be discovered automatically.

NetApp Host Agent does not initiate any actions that affect DataFabric Manager, the non-NetApp host, or related devices. It is strictly a passive agent that acts on requests from external management applications, such as DataFabric Manager.

What NetApp Host Agent can do

After NetApp Host Agent installed on a non-NetApp host, you can use DataFabric Manager to perform a variety of SAN and Storage Resource Management (SRM) functions.

SAN capabilities: Using NetApp Host Agent and DataFabric Manager, you can perform the following SAN tasks:

- ◆ Monitor basic system information for the SAN hosts
- ◆ View detailed HBA and LUN information

See Chapter 3, “[Using the NetApp Host Agent for SAN](#),” on page 13 for more information about NetApp Host Agent and SANs.

SRM capabilities: Using NetApp Host Agent and DataFabric Manager, you can perform the following SRM tasks:

- ◆ Collect storage usage data at the file and directory level
- ◆ Identify a variety of file-related information, for example, largest files, oldest files, or space consumed per file type

See Chapter 2, “[Using the NetApp Host Agent for SRM](#),” on page 5 for more information about NetApp Host Agent and SRM.

**When you need
NetApp Host Agent**

You need NetApp Host Agent *only* if you want to use DataFabric Manager to monitor SAN hosts or SRM data.

**Accessing NetApp
Host Agent**

The user interface to NetApp Host Agent is web-based. You can access it from the machine on which NetApp Host Agent is installed, or from any other machine on the network. See “[Accessing the user interface](#)” on page 23 for more information.

About this chapter

This chapter provides an overview of the SRM Host Agent and describes how you can use it to display SRM data in DataFabric Manager.

Topics in this chapter

This chapter contains the following topics:

- ◆ [“Prerequisites for SRM”](#) on page 6
- ◆ [“About SRM”](#) on page 8
- ◆ [“About NetApp Host Agent for SRM”](#) on page 10

Before reading further

This chapter provides an introduction to the DataFabric Manager SRM feature and its interaction with the NetApp Host Agent software. See the SRM chapter in the *DataFabric Manager Administration Guide* for additional important information.

Prerequisites for SRM

Prerequisites

You must meet the following prerequisites to use the DataFabric Manager SRM feature:

- ◆ You must have a valid SRM license installed on your DataFabric Manager management station. Contact your Network Appliance sales representative or the Installed Base Group (ibg@netapp.com) to obtain an SRM license.

Note

The Quotas subtab is visible in the DataFabric Manager user interface (under the Control Center > Home > Group Status tabs) until you install the Storage Resource Management license. After you install the license, the Quotas subtab is renamed to “SRM,” and all of the SRM features become visible when you click it.

- ◆ All hosts to be managed by DataFabric Manager must be connected to a TCP/IP network either known to or discoverable by DataFabric Manager. The hosts must be connected to the network through an Ethernet port and must have a valid IP address.
- ◆ All directory paths to be monitored must be visible to the host agent. For example, to enable DataFabric Manager SRM filer monitoring, the host agent must mount a filer share using NFS or CIFS, or the host agent must use a LUN on the filer.
- ◆ Before setting up SRM paths and schedules, you must enable host agent administrative access. See “[Administration settings that you must configure](#)” on page 6 and the *DataFabric Manager Administration Guide* for more information.

Administration settings that you must configure

You must enable administrative access to your host agents before you can perform SRM tasks with them. To enable administrative access, you must ensure that the passwords specified on DataFabric Manager match those set for the NetApp Host Agent software. The following table describes the options that must be set to enable administrative access.

Access type	DataFabric Manager options	NetApp Host Agent Software option
Monitoring only	Host Agent Login=guest Host Agent Monitoring Password	Monitoring API Password
Management	Management Host Agent Login=admin Host Agent Management Password	Management API Password

For more information about the NetApp Host Agent software passwords, see [“About the NetApp Host Agent software passwords”](#) on page 25.

About SRM

Definition of SRM

SRM is the monitoring and management of storage resources, including applications, files, file systems, and networks. DataFabric Manager interacts with the NetApp Host Agent software residing on remote Windows, Solaris, or Linux hosts (called *host agents*) to recursively examine the directory paths you have specified in the SRM configuration options. The results of these directory examinations are used to generate a variety of useful file-level and directory-level reports.

Does SRM monitor filers?

DataFabric Manager can monitor only directory paths that are visible to the host agent. Therefore, if you want to enable DataFabric Manager SRM filer monitoring, the host agent must mount a filer share using NFS or CIFS, or the host agent must use a LUN on the filer. DataFabric Manager cannot obtain SRM data for files located in filer volumes that are not exported by CIFS or NFS. Host agents can also gather SRM data about other file system paths that are not on a filer, for example, local disk and third-party storage. For more information about SRM prerequisites, see [“Prerequisites for SRM”](#) on page 6.

What if I want to view a file system on an unsupported platform?

As long as the file system is viewable from the host agent, you can retrieve data from it. For example, you can view files located on an HP/UX system, if the file system is NFS mounted on a Solaris box running the NetApp Host Agent Software.

Why you might need SRM

As companies expand their distributed computing systems and implement disaster recovery solutions, their storage requirements increase proportionately. As more storage devices are added to the network to fulfill these requirements, it becomes increasingly more difficult to determine how storage space is being allocated. What files types are taking up the most space? Which users are exceeding their quota limits? What are the 10 largest directories?

For example, if an administrator suspects that mp3 files are consuming an excessive amount of storage space on the network, how can he gather statistics for specific file extensions from the devices he is concerned about? Or perhaps an administrator wants to archive rarely used files. How can she generate a report listing the least-used files?

To keep costs down, and to proactively manage their storage networks, companies require an efficient way to determine how space is being used on their networks. Thus, the need for Storage Resource Management (SRM) tools. NetApp's SRM functionality enables you to gather file-level statistics and directory-centric SRM data.

SRM terminology you should know

Before you configure the DataFabric Manager and NetApp Host Agent software to gather SRM data, you should be familiar with the following SRM terms and technologies:

- ◆ SRM path
- ◆ SRM path “walk”

SRM path: A directory path defined by an administrator for the purpose of gathering file-level statistics, for example, oldest files, largest files, oldest files.

Path walk: The process of recursively examining a directory path for file-level statistics. The path walk is scheduled on DataFabric Manager and executed by the NetApp Host Agent software. The NetApp Host Agent software “walks” the specified directory path and gathers per-file and per-directory data.

About NetApp Host Agent for SRM

About the NetApp Host Agent for SRM hosts

NetApp Host Agent resides on each SRM host that you want to monitor through DataFabric Manager. You can use the NetApp Host Agent SRM functionality for both SAN and non-SAN hosts.

SRM management tasks you can perform with NetApp Host Agent

NetApp Host Agent enables you to perform the following SRM functions through DataFabric Manager:

- ◆ Set up path walk schedules for collecting file-level storage usage statistics
- ◆ Identify file-level statistics, such as
 - ❖ Largest files
 - ❖ Oldest files
 - ❖ Stalest files
 - ❖ Newest files
 - ❖ Largest directories
 - ❖ Files by owner
 - ❖ Files by type

Overview of SRM configuration

To begin gathering file-level information, you need to perform the following tasks.

1. Identify SRM host agents.

If you have installed an SRM license, all host agents will be automatically discovered by DataFabric Manager.
2. Add new host agents manually in DataFabric Manager, if they have not been discovered.
3. Set up host agent administrative access on the hosts to be monitored.

You must enable administrative access to your host agents before you can perform SRM tasks with them.
4. Verify NetApp Host Agent software administrative access.
5. Add SRM paths in DataFabric Manager.

After host agents have been discovered, you must define SRM paths on them.

6. Set up SRM path-walk schedules in DataFabric Manager.

You must define the interval between SRM path walks.

Note

SRM path walks can cause performance degradation. However, you can schedule your SRM path walks to occur during low-use or nonbusiness hours. See Chapter 2, “[Using the NetApp Host Agent for SRM](#),” on page 5 for more information.

You can begin collecting basic SRM data by completing the preceding tasks. The SRM path walks will begin according to the schedules you create. These configuration steps are described in detail in the *DataFabric Manager Administration Guide*.

Where to find more information

For more information, see the SRM chapter in the *DataFabric Manager Administration Guide*.

About this section This chapter provides an overview of the NetApp Host Agent and describes how it functions in a NetApp SAN.

Topics in this section This section contains information about the following topics:

- ◆ [“Assumptions”](#) on page 14
- ◆ [“How NetApp Host Agent functions in a SAN”](#) on page 16

Assumptions

Required reading

Before installing NetApp Host Agent, you should be familiar with the information about setting up a NetApp SAN in the *Data ONTAP Block Access Management Guide*.

SAN terminology that you should know

Before you configure DataFabric Manager and NetApp Host Agent to monitor your SAN, you should be familiar with the following SAN terms and technologies:

- ◆ SAN host
- ◆ Fibre Channel Protocol (FCP)
- ◆ Internet SCSI (iSCSI)
- ◆ Host Bus Adapter (HBA)
- ◆ SAN hosts
- ◆ Target
- ◆ Initiators
- ◆ Logical Unit Number (LUN)

SAN host: A SAN host is a SAN device, such as a UNIX or Windows system, that sends requests to other SAN devices in a SAN to perform tasks. To be monitored by DataFabric Manager, a SAN Host must be running the NetApp Host Agent software.

Fibre Channel Protocol (FCP): Fibre Channel is one of the storage networking protocols used by devices in a SAN to communicate with each other.

Internet SCSI (iSCSI): Internet SCSI (Small Computer System Interface) is an Internet Protocol (IP)-based storage networking protocol that enables communication between devices in a SAN over the ubiquitous IP networks.

Host bus adapter (HBA): A host bus adapter is an interface card that plugs into a SAN device. SAN devices use the ports on their respective HBAs to connect to each other in a SAN.

Each SAN device might contain one or more HBAs. An HBA might contain more than one port. Each port can be used to establish a connection to a SAN.

Initiators: An initiator (also known as a host bus adapter port or simply an HBA port) is an HBA port on a SAN host that is used to initiate requests to a filer in a NetApp SAN.

Target: A target is an HBA port on a filer in a NetApp SAN to which SAN hosts send requests.

Logical Unit Number (LUN): A LUN is a logical unit of storage on a filer (also known as a target) that is accessed by UNIX or Windows hosts (also known as SAN hosts) in a SAN.

How NetApp Host Agent functions in a SAN

About the NetApp Host Agent for SAN hosts

NetApp Host Agent resides on each SAN host that you want to monitor through DataFabric Manager.

In a SAN environment, NetApp Host Agent is a network interface to HBA and LUN management utilities on a SAN host. It enables you to monitor and manage SAN hosts from DataFabric Manager in a secure and platform-independent way.

SAN management tasks you can perform with NetApp Host Agent

NetApp Host Agent enables you to perform the following SAN functions through DataFabric Manager:

- ◆ Discover SAN hosts
- ◆ Monitor basic system information for the SAN host
- ◆ View detailed HBA port (initiator) information and some iSCSI HBA details
- ◆ View current LUN mappings on the SAN host
- ◆ Execute basic LUN management requests, including the following:
 - ❖ Create and map a LUN
 - ❖ Expand a LUN
 - ❖ Delete a LUN

Note

LUN management is available only on SAN hosts running Windows. It also requires awareness of SAN host clustering. NetApp Host Agent on hosts running Windows obtains clustering information from Microsoft Cluster Services. NetApp Host Agent on hosts running Solaris® and Linux cannot perform LUN management because it is not aware of SAN host clustering.

Flow of information through NetApp Host Agent

On Solaris and Linux: For HBA monitoring, and for LUN monitoring on SAN hosts running Solaris or Linux, NetApp Host Agent obtains monitoring and management information from the operating system and device drivers on the SAN host.

On Windows: For LUN monitoring and management on SAN hosts running Windows, NetApp Host Agent obtains data from SnapDrive. This data includes the following types of information:

- ◆ A list of LUNs
- ◆ The cluster configuration for SAN hosts (MS Server Cluster)
- ◆ The version of SnapDrive

NetApp Host Agent uses proprietary APIs to communicate this data to DataFabric Manager over an HTTP or HTTPS connection.

About this chapter

This chapter describes the system requirements for installing the NetApp Host Agent and describes how to obtain NetApp Host Agent 2.3 and install it on Windows, Solaris, and Linux hosts.

This chapter includes the following topics

- ◆ [“System requirements”](#)
- ◆ [“Obtaining and installing the NetApp Host Agent”](#)

System requirements

You must meet the following requirements before installing the NetApp Host Agent software.

NetApp Host Agent 2.3	
Windows servers	◆ Windows 2000 ◆ Windows XP ◆ Windows 2003
Solaris servers	◆ Solaris® 8, Solaris 9, and Solaris 10 running on UltraSPARC
Linux workstation or server	◆ Red Hat™ Enterprise Linux® ES for x86, version 3 (update 3 or later) ◆ Red Hat Enterprise Linux AS, version 3 (update 3 or later) ◆ SuSE® Linux Enterprise Server 9 Other Linux versions and distributions are not supported.
SnapDrive compatibility requirements (for supporting LUN management of Windows SAN hosts):	◆ version 3.0 ◆ version 3.0R1 ◆ version 3.0R2 ◆ version 3.1 ◆ version 3.1R1 ◆ version 3.2 ◆ version 4.0

Obtaining and installing the NetApp Host Agent

You can obtain the NetApp Host Agent 2.3 from the NOW site at <http://now.netapp.com>. Follow the installation instructions on the NOW site.

About this chapter This chapter describes how to use NetApp Host Agent to enable DataFabric Manager to monitor SAN hosts.

Topics in this chapter This chapter contains the following topics:

- ◆ “[Starting and stopping the NetApp Host Agent service](#)” on page 22
- ◆ “[Accessing the user interface](#)” on page 23
- ◆ “[User privileges and security](#)” on page 24
- ◆ “[Configuring NetApp Host Agent](#)” on page 25
- ◆ “[The NetApp Host Agent log file](#)” on page 28

Starting and stopping the NetApp Host Agent service

Starting and stopping on Windows

On Windows hosts, NetApp Host Agent runs as a service that starts automatically when the system boots up. You can start and stop NetApp Host Agent through the Services window, similar to other Windows services.

Starting and stopping on UNIX

On Solaris and Linux hosts, NetApp Host Agent is a daemon that is started by the `init` service.

You can also start and stop the daemon manually, as follows:

- ◆ To start the daemon, run the command `ntap_agent start`.
- ◆ To stop the daemon, run the command `ntap_agent stop`.

Multiple instances of NetApp Host Agent

In either Windows, Solaris, or Linux, when NetApp Host Agent starts, it detects whether another instance of NetApp Host Agent is running. It will not run more than one instance at the same time.

Accessing the user interface

User interface

The user interface to NetApp Host Agent is web-based. You can access it from the machine on which NetApp Host Agent is installed, or from any other machine on the network.

Addresses for accessing the user interface

Enter the following URLs in your browser to access the NetApp Host Agent user interface:

- ◆ To access configuration options, enter
[hostname or IP address]:[port]/admin
- ◆ To access diagnostic information, enter
[hostname or IP address]:[port]/about

Port information

NetApp Host Agent by default listens for HTTP requests on port 4092 and for HTTPS requests on port 4093. For information about HTTPS, see “[User privileges and security](#)” on page 24.

User privileges and security

User privilege levels

NetApp Host Agent supports two levels of user privilege: monitoring and management.

- ◆ Monitoring privileges enable you to perform only monitoring functions.
- ◆ Management privileges enable you to perform both monitoring and management functions.

User passwords in new installations

In new installations of NetApp Host Agent, the default password for the monitoring user is “public.”

New installations of NetApp Host Agent disable management access until a password is configured for it. For instructions on changing configuration options, see “[Configuring NetApp Host Agent](#)” on page 25.

Password security

Passwords are stored on the host in a strongly hashed format. Lost passwords cannot be recovered, but they can be reset by a user with administrator or root privileges on the host.

HTTPS transport

Whenever possible, NetApp Host Agent uses HTTPS transport to protect transmitted data and login information.

If DataFabric Manager is configured to use HTTP, communication between the DataFabric Manager and NetApp Host Agent will occur, but will be unencrypted.

Configuring NetApp Host Agent

Credential requirement

To change configuration options in NetApp Host Agent, you must supply valid administrator (super-user) credentials on the host. On Windows hosts, you must log in as an “Administrator” and on Solaris and Linux hosts you must log in as “root.”

About the NetApp Host Agent software passwords

Host agents have two user name and password pairs. One password is for monitoring only and the other password is for administration.

Monitoring password pair: The default monitoring password pair is as follows:

- ◆ User name=`guest`
- ◆ Password=`public`

Host agents have the preceding settings enabled by default. DataFabric Manager has been configured to recognize the password `public` so that read-only operations can be performed on host agents without further configuration. If you later decide to change the guest password on the host agent, you must then set the same user name and password in DataFabric Manager using the Host Agent Monitoring Password option on the Options page (banner > Options link).

Administration password pair: The administration password pair is as follows:

- ◆ User name=`admin`
- ◆ Password=`userspecified`

You specify the password on the host agent's configuration user interface (<http://name-of-agent:4092/>). This password pair allows read-write access to the host agent. After setting the administration password pair in the host agent, you must then set the same user name and password in DataFabric Manager using the following options:

- ◆ Host Agent Login
- ◆ Host Agent Management Password

These options are located on the Options page (banner > Options link) or the Edit Settings page (*appliance name* > Tools list > Edit Settings) of the individual host agent.

For more information, see Chapter 5, “[Using NetApp Host Agent](#),” on page 21.

Configuration options

The following table lists the configuration options and their functions.

Configuration option	Function	Default value
Monitoring API Password	Changes the password for the “guest” user.	public
Management API Password	Changes the password for the “admin” user.	Disabled
HTTP Port	Changes the port on which NetApp Host Agent always listens for requests.	4092
HTTPS Port	Changes the additional port on which NetApp Host Agent listens for requests if HTTPS is enabled.	4093
Remote Upgrade	Enables or disables remote upgrading of NetApp Host Agent. (To be supported in a future version of DataFabric Manager)	Disabled

Changing configuration options

To change configuration options in NetApp Host Agent, complete the following steps.

Step	Action
1	Access the NetApp Host Agent user interface from your browser.
2	At the login prompt, log in as the administrator or super-user. Note _____ For new installations, configure the management password if it has not already been configured. See “ User privileges and security ” on page 24. _____
3	Change options as needed.

Step	Action
4	Click Update.
5	Close the browser window to log out.

The NetApp Host Agent log file

Log file name and location

NetApp Host Agent maintains a single log file, named `ntap_agent.log`. The log file is located in the installation directory. The default installation directory locations are as follows:

- ◆ On Windows, `C:\Program Files\Network Appliance\Agent`
- ◆ On Solaris or Linux, `/opt/NTAPagent`

Log file size and rotation

Log files are rotated when the file size exceeds 3 MB. After a log has been rotated three times, it is deleted. The total combined size of all log files does not exceed 12 MB.