

NetApp Host Agent 2.5

Installation and Administration 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 215-03308_A0
August 2007

Copyright and trademark information

Copyright information

Copyright © 1994–2007 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

No part of this file 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.

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

THIS SOFTWARE IS PROVIDED BY NETWORK APPLIANCE “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 NETWORK APPLIANCE 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.

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.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication or disclosure by the government is subject to restrictions 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, FlexClone, FlexVol, Manage ONTAP, MultiStore, NearStore, NetCache, SecureShare, SnapDrive, SnapLock, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapValidator, SnapVault, Spinnaker Networks, SpinCluster, SpinFS, SpinHA, SpinMove, SpinServer, SyncMirror, Topio, VFM, and WAFL are registered trademarks of Network Appliance, Inc. in the U.S.A. and/or other countries. Cryptainer, Cryptoshred, Datafort, and Decru are registered trademarks, and Lifetime Key Management and OpenKey are trademarks, of Decru, a Network Appliance, Inc. company, in the U.S.A. and/or other countries. gFiler, Network Appliance, SnapCopy, Snapshot, and The evolution of storage are trademarks of Network Appliance, Inc. in the U.S.A. and/or other countries and registered trademarks in some other countries. ApplianceWatch, BareMetal, Camera-to-Viewer, ComplianceClock, ComplianceJournal, ContentDirector, ContentFabric, EdgeFiler, FlexShare, FPolicy, HyperSAN, InfoFabric, LockVault, NOW, NOW NetApp on the Web, ONTAPI, RAID-DP, RoboCache, RoboFiler, SecureAdmin, Serving Data by Design, SharedStorage, Simplicore, Simulate ONTAP, Smart SAN, SnapCache, SnapDirector, SnapFilter, SnapMigrator, SnapSuite, SohoFiler, SpinMirror, SpinRestore, SpinShot, SpinStor,

StoreVault, vFiler, Virtual File Manager, VPolicy, and Web Filer are trademarks of Network Appliance, Inc. in the U.S.A. and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of Network Appliance, Inc. in the U.S.A.

IBM, the IBM logo, AIX, and System Storage are trademarks and/or registered trademarks of International Business Machines Corporation.

Apple is a registered trademark and QuickTime is a trademark of Apple Computer, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. 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 U.S.A. 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	vii
Chapter 1	Overview NetApp Host Agent	1
	Before reading further	2
	How NetApp Host Agent works	3
Chapter 2	Using NetApp Host Agent with FSRM.	5
	Prerequisites for File Storage Resource Manager	6
	About File Storage Resource Manager	8
	Overview of NetApp Host Agent with FSRM	10
Chapter 3	Using NetApp Host Agent for a SAN	13
	Prerequisites for NetApp Host Agent for a SAN	14
	How NetApp Host Agent functions in a SAN	16
Chapter 4	Installing NetApp Host Agent	19
	System requirements	20
	Installing NetApp Host Agent on Windows, Solaris, or Linux	22
	Uninstalling NetApp Host Agent	23
Chapter 5	Managing NetApp Host Agent	25
	Starting and stopping the NetApp Host Agent service	26
	Accessing the user interface	27
	User privileges and security	28
	Configuring NetApp Host Agent	29
	NetApp Host Agent log file	32
	Index	33

Preface

About this guide

You can use the NetApp® Host Agent software to monitor hosts through the DataFabric Manager and the Operations Manager interface. This guide describes how to install this software on a Windows®, Solaris®, or Linux® host.

This guide does not cover basic system or network administration topics, such as IP addressing and network management; it emphasizes the preparations and product installation that you should carry out on hosts to enable their monitoring by the DataFabric Manager server.

Audience

This guide is for system administrators and others interested in monitoring hosts through DataFabric Manager and the Operations Manager interface.

This guide assumes that you are familiar with the following:

- ◆ Data ONTAP operating system software
- ◆ Protocols (NFS, CIFS, or HTTP) you use for file sharing or transfers
- ◆ Client-side operating systems (UNIX® or Windows®)

Terminology conventions

Storage systems that run Data ONTAP are referred to as *storage systems*, *filers*, *appliances*, *storage appliances*, or *systems*. The terms used in the graphical user interface for Operations Manager reflect these common usages.

When the term *appliance* is used in Operations Manager, the information applies to all supported storage systems, NearStore® systems, FAS appliances, and in some cases Fibre Channel switches.

When the term *filer* is used, it can refer to any supported storage system, including FAS appliances or NearStore systems.

Windows-based, Linux-based, and Solaris-based storage systems that do not run Data ONTAP are referred to as *hosts*.

Path convention

In parenthetical references to paths leading to parts of the Operations 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 > Tools > Options means to click the File Systems tab, open the Tools drop-down list, and select Options.

Command conventions

You can enter storage system commands on the system console or from any client that can obtain access to the storage system using a Telnet session. In examples that illustrate commands executed on a UNIX workstation, the command syntax and output might differ from what you actually see on your system, depending on your version of UNIX.

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, the guide might say to enter the following command: <code>dfm alarm destroy alarm-ids</code> You must 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.

Keyboard conventions

This guide uses capitalization and some abbreviations to refer to the keys on the keyboard. The keys on your keyboard might not be labeled exactly as they are in this guide.

What is in this guide...	What it means...
hyphen (-)	Used to separate individual keys. For example, Ctrl-D means holding down the Ctrl key while pressing the D key.

What is in this guide...	What it means...
<i>Enter</i>	Used to refer to the key that generates a carriage return; the key is named Return on some keyboards.
<i>type</i>	Used to mean pressing one or more keys on the keyboard.
<i>enter</i>	Used to mean pressing one or more keys and then pressing the Enter key.

Special messages

This guide contains special messages that are described as follows:

Note

A note contains information that is important for you to consider as you work with the information in this guide.

Attention

An attention notice contains instructions that you must follow to avoid a system crash, loss of data, or damage to the equipment.

About this chapter This chapter provides an overview of the NetApp Host Agent software.

Topics in this chapter This chapter 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
- ◆ Operations Manager
- ◆ SAN host
- ◆ File Storage Resource Manager (FSRM)
- ◆ SnapDrive® software
- ◆ Microsoft Cluster Services (MSCS)

NetApp Host Agent: This independent software agent resides on any third-party (Windows®, Solaris™, or Linux®) host that you want to monitor through the NetApp Operations Manager interface to the DataFabric Manager server.

Host agent: This is a server running the NetApp Host Agent software. If the host agent has SAN hardware, it can also be referred to as a *SAN host*.

Operations Manager: This Web-based interface to the DataFabric Manager server lets you monitor or manage NetApp storage systems or Windows, Solaris, or Linux systems installed with NetApp Host Agent.

SAN host: This is any 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 through Operations Manager on the DataFabric Manager server, a SAN host must be running the NetApp Host Agent software.

File Storage Resource Manager (FSRM): This feature on the DataFabric Manager server enables you to monitor and manage file-level and directory-centric storage resource management (SRM) data on hosts installed with NetApp Host Agent.

SnapDrive: This software configures space on NetApp storage systems as local disks on Windows hosts. SnapDrive is required for LUN management when NetApp Host Agent is providing the SAN host functionality on Windows.

Microsoft Cluster Services (MSCS): This 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 NetApp Host Agent

NetApp Host Agent is software that resides on a Windows, Linux, or Solaris host. It collects information such as OS name, version, HBA information, and file-system metadata, and then sends that information back to the DataFabric Manager server. Users can create reports of the collected information by using Operations Manager or the DataFabric Manager CLI.

To enable a target host to communicate with the DataFabric Manager server, install and configure the NetApp Host Agent software on that host. After the DataFabric Manager server discovers that instance of NetApp Host Agent, no further configuration is required.

NetApp Host Agent does not initiate any management actions on the Windows, Linux, or Solaris host. It is strictly a passive agent. It acts only on requests from external management applications, such as the DataFabric Manager server.

What NetApp Host Agent Can Do

After you install NetApp Host Agent on a Windows, Linux, or Solaris host, you can use Operations Manager to perform a variety of SAN and FSRM functions.

SAN capabilities: Using NetApp Host Agent and Operations 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 NetApp Host Agent for a SAN](#),” on page 13 for more information about NetApp Host Agent and SANs.

FSRM capabilities: Using NetApp Host Agent and Operations Manager, you can perform the following FSRM 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 NetApp Host Agent with FSRM](#),” on page 5 for more information about NetApp Host Agent and FSRM.

**When you need
NetApp Host Agent**

You need NetApp Host Agent *only* if you want to monitor SAN hosts or FSRM-generated file system data through Operations Manager.

**Accessing NetApp
Host Agent**

NetApp Host Agent uses a Web-based interface for configuration. You can access it either 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 27 for more information.

About this chapter

This chapter provides an overview of how to use NetApp Host Agent to display File Storage Resources Manager (FSRM) data through Operations Manager.

Topics in this chapter

This chapter contains the following topics:

- ◆ [“Prerequisites for File Storage Resource Manager”](#) on page 6
- ◆ [“About File Storage Resource Manager”](#) on page 8
- ◆ [“Overview of NetApp Host Agent with FSRM”](#) on page 10

Before reading further

This chapter introduces the File Storage Resource Manager feature of Operations Manager and its interaction with the NetApp Host Agent software. See the File Storage Resource Manager chapter in the *DataFabric Manager with Operations Manager Administration Guide* for additional important information.

Prerequisites for File Storage Resource Manager

Prerequisites

You must meet the following prerequisites to use the Operations Manager FSRM feature:

- ◆ You must have a valid FSRM license installed on your DataFabric Manager server. Contact your sales representative or the Installed Base Group (ibg@netapp.com) to obtain a File SRM license.

Note

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

- ◆ All hosts to be managed through Operations Manager must be connected to a TCP/IP network either known to or discoverable by the DataFabric Manager server. 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 FSRM host monitoring by the DataFabric Manager server, the host agent must mount a storage system share using NFS or CIFS, or the host agent must use a LUN on the storage system.
- ◆ Before setting up FSRM paths and schedules, you must enable host agent administrative access. See “[Administration settings that you must configure](#)” on page 6 and the *DataFabric Manager with Operations 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 FSRM tasks with them. To enable administrative access, you must ensure that the passwords specified on the DataFabric Manager server match those set in the NetApp Host Agent software. The following table describes the options that must be set to enable administrative access.

Access type	Operations 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 29.

About File Storage Resource Manager

Definition of FSRM

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

Does FSRM monitor NetApp storage systems?

Through Operations Manager, you can monitor only directory paths that are already visible to the NetApp Host Agent software. Therefore, if you want to enable FSRM monitoring of a NetApp storage system, the host agent must mount that storage system share using NFS or CIFS, or the host agent must use a LUN on that storage system.

Note

The DataFabric Manager server cannot obtain file system data for files located in a storage system's volumes that are not exported by CIFS or NFS. Host agents can also gather FSRM data about file system paths that are not on a storage system: for example, local disk and third-party storage. For more information about FSRM prerequisites, see "[Prerequisites for File Storage Resource Manager](#)" 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 host running the NetApp Host Agent software.

Why you might need FSRM

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 file types are taking up the most space? Which users are exceeding their quotas? What are the 10 largest directories?

For example, if an administrator suspects that MP3 files are consuming an excessive amount of storage resource space, how can that administrator gather statistics for specific file extensions from the affected devices? Alternatively, perhaps an administrator wants to archive rarely used files. How can that administrator generate a report listing the least-used files?

To keep costs down, and to manage proactively their storage resource space, companies require an efficient way to determine how that space is being used: thus, the need for the FSRM tools. FSRM enables you to gather file-level statistics and directory-centric file system data.

FSRM terminology you should know

Before you configure the Operations Manager and NetApp Host Agent software to gather FSRM-requested file system data, you should be familiar with the following SRM terms and technologies:

- ◆ Path
- ◆ Path walk

Path: Defined by an administrator, a directory path gathers file-level statistics (such as file listing by age, size, owner, or type).

Path walk: A “path walk” is the process of recursively examining a directory path for file-level statistics. You can schedule this process through Operations Manager and execute it through the NetApp Host Agent software. The NetApp Host Agent software then “walks” the specified directory path and gathers per-file and per-directory data.

Overview of NetApp Host Agent with FSRM

About NetApp Host Agent with FSRM

NetApp Host Agent resides on each FSRM host from which you want to collect file-system metadata. You can use NetApp Host Agent in conjunction with FSRM for both SAN and non-SAN hosts.

FSRM management tasks you can perform with NetApp Host Agent

NetApp Host Agent enables you to perform the following FSRM functions through Operations Manager:

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

Overview of FSRM configuration

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

1. Identify FSRM host agents.

If you have installed an FSRM license, DataFabric Manager will automatically discover all host agents.
2. Add new host agents manually in Operations 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 FSRM tasks with them.
4. Verify NetApp Host Agent software administrative access.
5. Add paths in Operations Manager.

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

6. Set up path-walk schedules in Operations Manager.

You must define the interval between path walks.

Note

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

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

Where to find more information

For more information, see the File Storage Resource Manager chapter in the *DataFabric Manager with Operations Manager Administration Guide*.

About this chapter

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

Topics in this chapter

This chapter contains information about the following topics:

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

Prerequisites for NetApp Host Agent for a SAN

Required reading

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

SAN terminology that you should know

Before you configure Operations Manager and NetApp Host Agent to monitor a 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)
- ◆ Target
- ◆ Initiators
- ◆ Logical unit number (LUN)

SAN host: A SAN host is a SAN device, such as a UNIX, LINUX, or Windows system, that sends requests to other SAN devices in a SAN to perform tasks. To be monitored by the DataFabric Manager server, 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 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.

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

Initiator: 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 storage system in a NetApp SAN.

Logical unit number (LUN): A LUN is a logical unit of storage on a storage system (also known as a *target*) that is accessed by UNIX, LINUX, or Windows hosts (also known as *SAN hosts*) in a SAN.

How NetApp Host Agent functions in a SAN

About NetApp Host Agent for SAN hosts

NetApp Host Agent resides on each SAN host that you want to monitor through Operations 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 through Operations 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 Operations 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 information:

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

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

About this chapter

This chapter describes the system requirements and steps for obtaining and installing NetApp Host Agent on Windows, Solaris, and Linux hosts.

This chapter includes the following topics:

- ◆ [“System requirements”](#)
- ◆ [“Installing NetApp Host Agent on Windows, Solaris, or Linux”](#)
- ◆ [“Uninstalling NetApp Host Agent”](#)

System requirements

The NetApp Host Agent software can be installed on supported versions of Windows, Solaris, Red Hat®, and SUSE® operating systems running on Windows, Solaris, and Linux workstations and servers.

Note

To check compatibility information for operating systems or software released after the production of this guide, view the *DataFabric Manager Support of NetApp Host Agent & SnapDrive for Windows* matrix on the NOW® site. See “[Viewing the most current system requirements](#)” on page 21.

Operating system or software	Versions compatible with NetApp Host Agent 2.5
Windows servers	◆ Windows 2000 ◆ Windows XP ◆ Windows 2003
Solaris servers	◆ Solaris 8 running on UltraSPARC ◆ Solaris 9 running on UltraSPARC ◆ Solaris 10 running on UltraSPARC
Linux workstation or server	◆ Red Hat Enterprise Linux ES, version 3 (32-bit, update 3 or later) ◆ Red Hat Enterprise Linux AS 3 (32-bit, update 3 or later) ◆ Red Hat Enterprise Linux AS 4 (32-bit and 64-bit) ◆ Red Hat Enterprise Linux ES, version 4 (32-bit, update 3 or later) ◆ SUSE Linux Enterprise Server 9 (32-bit and 64-bit, SP 2 or later)
SnapDrive for Windows (to support LUN management of Windows SAN hosts)	◆ SnapDrive 3.0, 3.0R1, 3.0R2, 3.1, 3.1.1R1, 3.2, 4.0, 4.1, 4.2, 4.2.1 and 5.0.

Viewing the most current system requirements: For the complete list of supported devices, operating systems, and SnapDrive for Windows versions, including those released after the production of this guide, see the *DataFabric Manager Support of NetApp Host Agent & SnapDrive for Windows* matrix on the NOW site.

To view the compatibility matrix, log in to the NOW site at <http://now.netapp.com> and select Service and Support > Technical Assistance and Documentation > Access and Order product documentation > DataFabric Manager Support Matrix > Support of Host Agent and SnapDrive for Windows.

Installing NetApp Host Agent on Windows, Solaris, or Linux

You can install NetApp Host Agent on your target host either by download from the NOW site or from the DataFabric Manager CD.

Obtaining and installing from the NOW site: To obtain and install NetApp Host Agent, log in to the NOW site at <http://now.netapp.com> and select Service and Support > Software Download > Download Software > NetApp Host Agent and follow the NOW site download and installation instructions.

Installing from the DataFabric Manager CD: If you are installing NetApp Host Agent from the DataFabric Manager CD onto a Windows, Solaris, or Linux host, complete the following steps.

Step	Action	
1	Ensure that your host meets the requirements described in “ System requirements ” on page 20.	
2	Insert the CD into the CD-ROM drive of your Windows, Solaris, or Linux host.	
3	If you are installing on...	Then launch...
	◆ Windows (any version)	agentsetup-2-5-win32.exe in the win32 directory on your CD
	◆ Solaris (any version)	agentsetup-2-5-solaris.sh in the Solaris directory on your CD
	◆ Red Hat Enterprise Linux ES or AS (any version) ◆ SUSE Linux Enterprise Server 9	agentsetup-2-5-linux.bin in the Linux directory on your CD
4	Follow the NetApp Host Agent setup prompts to complete the installation. During the installation, you must specify a license key. After the installation is complete, NetApp Host Agent is launched automatically.	

Uninstalling NetApp Host Agent

If you need to uninstall NetApp Host Agent, complete the steps appropriate to the platform from which you are removing it.

Platform	Uninstall steps
Solaris	Log in as root and enter the following command: pkgrm NTAPagent
Linux	Log in as root and enter the following command to invoke the uninstall script: /opt/NTAPagent/uninstall
Windows	Use the Windows Add/Remove programs utility.

About this chapter This chapter describes how to manage NetApp Host Agent so that you can monitor SAN hosts through Operations Manager.

Topics in this chapter This chapter contains the following topics:

- ◆ “[Starting and stopping the NetApp Host Agent service](#)” on page 26
- ◆ “[Accessing the user interface](#)” on page 27
- ◆ “[User privileges and security](#)” on page 28
- ◆ “[Configuring NetApp Host Agent](#)” on page 29
- ◆ “[NetApp Host Agent log file](#)” on page 32

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, as you would to other Windows services.

Starting and stopping on Solaris and LINUX

On Solaris and Linux hosts, NetApp Host Agent is a daemon 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 Windows, Solaris, or Linux, when NetApp Host Agent starts, it checks if another instance of NetApp Host Agent is running. If another instance of NetApp Host Agent is running, the second instance shuts down. No more than one instance can run 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 28.

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 29.

Password security

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

HTTPS transport

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

If Operations Manager is configured to use HTTP, communication between the DataFabric Manager server and NetApp Host Agent occurs but is 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 or any other member of a Local Administrator group and on Solaris/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 user name and password pair: The default monitoring user name and password pair is as follows:

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

Host agents have the preceding settings enabled by default. The DataFabric Manager server is 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 Operations Manager (Tools > Options), using the Host Agent Monitoring Password option on the Options page.

Administration user name and password pair: The administration user name and 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 user name and password pair allows read-write access to the host agent. After setting the administration user name and password pair in the host agent, you must then set the same user name and password in Operations Manager using the following options:

- ◆ Host Agent Login
- ◆ Host Agent Management Password

These options are located on the Options page of each host agent (from Operations Manager, select Tools > Options to get to the Options page).

For more information, see Chapter 5, “[Managing NetApp Host Agent](#),” on page 25.

Configuration options

The following table lists the configuration options and their functions.

Configuration option	Function	Default value
MonitoringAPI Password	Changes the password for the “guest” user	public
Management API Password	Changes the password for the “admin” user	Disabled
HTTP Port	Changes the additional port on which NetApp Host Agent listens for requests if HTTPS is enabled	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 (currently not supported)	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 28. _____

Step	Action
3	Change options as needed.
4	Click Update.
5	Close the browser window to log out.

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\NetApp\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.

Index

A

- about this guide vii
- accessing
 - NetApp Host Agent 4
- audience vii

C

- configuration
 - NetApp Host Agent 29
 - options 30
- conventions
 - commands viii
 - path vii
 - typographic viii

F

- Fibre Channel Protocol (FCP) 14
- File Storage Resource Manager (FSRM) 2
 - configuration 10
 - management 10

H

- Host bus adapter (HBA) 14
- HTTP port 30
- HTTPS
 - port 30
 - transport 28

I

- installation
 - NetApp Host Agent 22
- installation requirements
 - Windows 20
- interface
 - user 27
- Internet SCSI (iSCSI) 14

K

- Keyboard viii
- Keyboard conventions viii

L

- license key
 - for SRM 6
- Linux
 - based storage systems vii
 - hardware requirements 20
 - software requirements 20
- log file
 - NetApp Host Agent 32
- logical unit number (LUN) 15

O

- overview
 - NetApp Host Agent 1

P

- password
 - API management 30
 - API monitoring 30
 - Host Agent management 7
 - Host Agent monitoring 7
 - NetApp Host Agent software 29
 - new installation 28
 - on the DataFabric Manager 6
 - pair 29
 - security 28
- port information 27
- prerequisites
 - for SRM components 6
- privileges
 - user 28

R

- requirement

- credential 29
- requirements
 - for SRM 6

S

- SAN host 2, 14
- security 28
- services 26
- SnapDrive 2
- software requirements
 - Linux 20
 - Solaris 20
 - Windows 20
- Solaris
 - based storage systems vii
 - hardware requirements 20
 - software requirements 20
- special messages ix
- SRM
 - configuration 10

- prerequisites 6
- SRM license key 6
- system requirements 20

T

- Terminology conventions vii
- terms 2

U

- upgrade
 - remote 30

W

- Windows
 - based storage systems vii
 - hardware requirements 20
 - software requirements 20