

NetApp® Host Agent 2.7 Installation and Administration Guide

NetApp, 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: 215-04430_A0
Processed: Wednesday May 6 2009 11:32:33 PM

Contents

Copyright information.....	5
Trademark information.....	7
About this guide.....	9
Audience.....	9
Terminology.....	9
Command, keyboard, and typographic conventions.....	10
Special messages.....	11
Overview of NetApp Host Agent	13
What NetApp Host Agent is.....	13
NetApp Host Agent terminology.....	13
What NetApp Host Agent does.....	14
NetApp Host Agent with FSRM.....	17
Interaction between NetApp Host Agent and FSRM.....	17
FSRM terminology.....	18
What FSRM does.....	18
Features and limitations of FSRM.....	19
Prerequisites for using FSRM.....	19
Administrative access requirements for FSRM.....	20
Configuring FSRM.....	21
NetApp Host Agent in a SAN.....	23
NetApp Host Agent for SAN hosts.....	23
SAN terminology.....	24
Prerequisites for using NetApp Host Agent in a SAN.....	24
NetApp Host Agent information flow in a SAN.....	25
NetApp Host Agent installation.....	27
NetApp Host Agent system requirements.....	27
Operating systems that support NetApp Host Agent	27
Software versions that support NetApp Host Agent	28
Installing NetApp Host Agent	29
Installing NetApp Host Agent from the NOW site	29
Installing NetApp Host Agent from a CD.....	29
Uninstalling NetApp Host Agent	30

- NetApp Host Agent administration.....31**
 - Access to the user interface.....31
 - User privileges and security.....32
 - NetApp Host Agent passwords.....32
 - NetApp Host Agent configuration options.....33
 - Setting passwords in NetApp Host Agent 34
 - Modifying settings for DataFabric Manager service.....35
 - Starting and stopping the NetApp Host Agent service.....35
 - Regenerating the host agent ID number.....36
 - The NetApp Host Agent log file.....37
 - Limitations of NetApp Host Agent 37
 - Discovery on cloned systems.....37
 - Unresponsiveness with SnapDrive for Windows uninstall.....37
- Index.....39**

Copyright information

Copyright © 1994–2009 NetApp, 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.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP 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.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. 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 NetApp.

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 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

All applicable trademark attribution is listed here.

NetApp, the Network Appliance logo, the bolt design, NetApp-the Network Appliance Company, Cryptainer, Cryptoshred, DataFabric, DataFort, Data ONTAP, Decru, FAServer, FilerView, FlexClone, FlexVol, Manage ONTAP, MultiStore, NearStore, NetCache, NOW NetApp on the Web, SANscreen, SecureShare, SnapDrive, SnapLock, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapValidator, SnapVault, Spinnaker Networks, SpinCluster, SpinFS, SpinHA, SpinMove, SpinServer, StoreVault, SyncMirror, Topio, VFM, and WAFL are registered trademarks of NetApp, Inc. in the U.S.A. and/or other countries. gFiler, Network Appliance, SnapCopy, Snapshot, and The evolution of storage are trademarks of NetApp, Inc. in the U.S.A. and/or other countries and registered trademarks in some other countries. The NetApp arch logo; the StoreVault logo; ApplianceWatch; BareMetal; Camera-to-Viewer; ComplianceClock; ComplianceJournal; ContentDirector; ContentFabric; EdgeFiler; FlexShare; FPolicy; Go Further, Faster; HyperSAN; InfoFabric; Lifetime Key Management, LockVault; NOW; ONTAPI; OpenKey, RAID-DP; ReplicatorX; RoboCache; RoboFiler; SecureAdmin; Serving Data by Design; Shadow Tape; SharedStorage; Simplicore; Simulate ONTAP; Smart SAN; SnapCache; SnapDirector; SnapFilter; SnapMigrator; SnapSuite; SohoFiler; SpinMirror; SpinRestore; SpinShot; SpinStor; vFiler; VFM Virtual File Manager; VPolicy; and Web Filer are trademarks of NetApp, Inc. in the U.S.A. and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of NetApp, Inc. in the U.S.A.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>.

Apple is a registered trademark and QuickTime is a trademark of Apple, 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.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetCache is certified RealSystem compatible.

About this guide

Here you can learn what this document describes and who it is intended for. The section also describes what special terminology is used in the document, what command, keyboard, and typographic conventions this document uses to convey information.

This document describes how to install and configure the NetApp Host Agent software on a Windows, Solaris, or Linux host to monitor hosts through DataFabric Manager and the Operations Manager interface.

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

Next topics

[Audience](#) on page 9

[Terminology](#) on page 9

[Command, keyboard, and typographic conventions](#) on page 10

[Special messages](#) on page 11

Audience

Here you can learn who this document is written for and the assumptions that were made about the preexisting knowledge and experience you have.

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

This document assumes that you are familiar with the following technology:

- Data ONTAP operating system software
- The protocols you use for file sharing or transfers, such as NFS, CIFS, or HTTP
- The client-side operating systems (UNIX or Windows)

Terminology

To understand the concepts in this document, you might need to know the terms defined here.

General storage system terminology

- Storage systems that run Data ONTAP are sometimes referred to as *filers*, *appliances*, *storage appliances*, or *systems*. The name of the FilerView graphical user interface for Data ONTAP reflects one of these common usages.
- *Controller* or *storage controller* refers to the component of a storage system that runs the Data ONTAP operating system and controls its disk subsystem. Controllers or storage controllers are also sometimes called *storage appliances*, *appliances*, *storage engines*, *heads*, *CPU modules*, or *controller modules*.

Storage hardware terminology

- *FC HBA for Disk* or *FC HBA* refers to the Fibre Channel host bus adapter that connects the node to the switch or to the disks.
- *Disk shelf* refers to a unit of the disk subsystem component of the storage system.
- *ESH (Embedded Switching Hub)* disk shelf module refers to a component that provides a means of managing an FC-AL loop in an intelligent manner, such that a single drive failure does not take down the loop. It also contains the enclosure services processor, which communicates the environmental data of the disk shelf.
- *ESH2* disk shelf module refers to a second-generation ESH module.
- *ESH4* disk shelf module refers to a third-generation ESH module.
- *AT-FCX* refers to an enhanced FC-AL to Serial ATA (SATA) bridge used in some disk shelves.

General terms

- The term *type* means pressing one or more keys on the keyboard.
- The term *enter* means pressing one or more keys on the keyboard and then pressing the Enter key, or clicking in a field in a graphical interface and typing information into it.

Command, keyboard, and typographic conventions

This document uses command, keyboard, and typographic conventions that help you enter commands.

Command conventions

In examples that illustrate commands executed on a UNIX workstation, the command syntax and output might differ, depending on your version of UNIX.

Keyboard conventions

- When describing key combinations, this document uses the hyphen (-) to separate individual keys. For example, "Ctrl-D" means pressing the "Control" and "D" keys simultaneously.

- This document uses the term "Enter" to refer to the key that generates a carriage return, although the key is named "Return" on some keyboards.

Typographic conventions

The following table describes typographic conventions used in this document.

Convention	Type of information
<i>Italic font</i>	Words or characters that require special attention. Placeholders for information you must supply. For example, if the guide says to enter the <code>arp -d <i>hostname</i></code> command, you enter the characters "arp -d" followed by the actual name of the host. Book titles in cross-references.
Monospaced font	Command names, option names, keywords, 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.

Special messages

This document might contain the following types of messages to alert you to conditions you need to be aware of. Danger notices and caution notices only appear in hardware documentation, where applicable.

Note: A note contains important information that helps you install or operate the system efficiently.

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

Danger: A danger notice warns you of conditions or procedures that can result in death or severe personal injury.

Caution: A caution notice warns you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous.

Overview of NetApp Host Agent

You can use the NetApp Host Agent software to collect information about your storage system and forward that information to your DataFabric Manager server.

Next topics

[What NetApp Host Agent is](#) on page 13

[NetApp Host Agent terminology](#) on page 13

[What NetApp Host Agent does](#) on page 14

What NetApp Host Agent is

NetApp Host Agent is software that resides on a Windows, Linux, or Solaris host. You need NetApp Host Agent only if you want to monitor SAN hosts or FSRM-generated file system data through Operations Manager.

The NetApp Host Agent software collects information such as operating system name, version, HBA port details, and file-system metadata, and then sends that information to a DataFabric Manager server. You can create reports using the information that NetApp Host Agent collects 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 the NetApp Host Agent software, 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.

Note: NetApp Host Agent 2.7 and later supports not only IPv4 but also IPv6.

NetApp Host Agent terminology

Before reading further about the NetApp Host Agent software, familiarize yourself with these terms and technologies.

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

File Storage Resource Manager (FSRM)	This feature in Operations Manager enables you to monitor and manage file-level and directory-centric Storage Resource Management (SRM) data on hosts installed with the NetApp Host Agent software.
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 the NetApp Host Agent software.
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.
SnapDrive	This software configures space on NetApp storage systems as local disks. 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.

What NetApp Host Agent does

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

NetApp Host Agent can perform monitoring operations for FSRM and for SAN storage environments.

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

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

Related concepts

[*NetApp Host Agent with FSRM*](#) on page 17

[*NetApp Host Agent in a SAN*](#) on page 23

NetApp Host Agent with FSRM

The File Storage Resource Manager (FSRM) feature of Operations Manager interacts with the NetApp Host Agent software to monitor directory paths and collect file-system metadata.

See the File Storage Resource Manager chapter in the *Operations Manager Administration Guide* for additional important information.

Next topics

[Interaction between NetApp Host Agent and FSRM](#) on page 17

[FSRM terminology](#) on page 18

[What FSRM does](#) on page 18

[Features and limitations of FSRM](#) on page 19

[Prerequisites for using FSRM](#) on page 19

[Administrative access requirements for FSRM](#) on page 20

[Configuring FSRM](#) on page 21

Related information

[Operations Manager Administration Guide -](#)

http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel371/.

Interaction between NetApp Host Agent and 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 to recursively examine the directory paths you have specified in the Operations Manager FSRM configuration options. The NetApp Host Agent software resides on remote Windows, Solaris, or Linux hosts. The results of these directory examinations are used to generate a variety of useful file-level and directory-level reports.

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

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

See the *Operations Manager Administration Guide* for more information about File Storage Resource Manager.

Related information

Operations Manager Administration Guide -
http://now.netapp.com/NOW/knowledge/docs/DFM_win/rel371/.

FSRM terminology

Before configuring Operations Manager and the NetApp Host Agent software to gather FSRM-requested file system data, familiarize yourself with these FSRM terms and technologies.

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.

What FSRM does

FSRM enables you to gather file-level statistics and directory-centric file system data so that you can monitor and manage storage space efficiently.

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, imagine that an administrator suspects that MP3 files are consuming an excessive amount of storage resource space. The administrator assesses the following factors:

- How to gather statistics for specific file extensions from the affected devices?

Note: An administrator might want to archive rarely used files.

- How to generate a report listing the least-used files?

Using FSRM tools enables you to do the following:

- Evaluate storage space usage.
- Keep costs down.
- Manage storage resource space.
- Gather file-level statistics and directory-centric file system data.

Features and limitations of FSRM

Using the FSRM feature of Operations Manager, you can use NetApp Host Agent to monitor storage systems and view file system details on unsupported platforms. However, you can monitor only directory paths that are already visible to the NetApp Host Agent software.

Monitoring storage systems

Through Operations Manager, you can monitor only directory paths that are already visible to the NetApp Host Agent software. FSRM monitoring of a storage system can be enabled by one of the following two ways:

- The host agent must mount that storage system share using NFS or CIFS
- The host agent must use a LUN on that storage system

Note: If volumes in a storage system are not exported by CIFS or NFS, the DataFabric Manager server cannot obtain file system data for files located in those volumes. 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.

Viewing 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.

Prerequisites for using FSRM

To use the FSRM feature, you must first install a valid FSRM license on your DataFabric Manager server.

Following are the prerequisites for using FSRM:

- A valid FSRM license must be installed on your DataFabric Manager server.
Contact your sales representative or the Installed Base Group (ibg@netapp.com) to obtain a license.
- 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, implement either of the following methods:
 - The host agent must be mounted on a storage system share using NFS or CIFS
 - The host agent must use a LUN on the storage system
- Before setting up FSRM paths and schedules, administrative access must be enabled to your host agents.

Related references

[Administrative access requirements for FSRM](#) on page 20

Administrative access requirements for FSRM

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

Related concepts

[NetApp Host Agent passwords](#) on page 32

Configuring FSRM

To begin gathering file-level information, you need to configure FSRM. The configuration steps are described in detail in the *Operations Manager Administration Guide*.

Before you begin

Following are the prerequisites to configuring FSRM:

- Identify the FSRM host agents you want to monitor.
- Set up administrative access on the identified FSRM host agents.
- Enable administrative access to your host agents before you can perform FSRM tasks with them.

Steps**1. Add FSRM host agents.**

If you have installed an FSRM license, DataFabric Manager automatically discovers all host agents on its local network, otherwise you can add new host agents manually in Operations Manager or configure host-initiated discovery so that the host agents can automatically register themselves with DataFabric Manager.

Note: Host-initiated discovery is a new feature in NetApp Host Agent 2.7. Host-initiated discovery is described in detail in the *Operations Manager Administration Guide*.

- 2. Set up administrative access for the NetApp Host Agent software.**
- 3. Define paths to the host agents in Operations Manager.**

The procedure for adding paths is described in detail in the *Operations Manager Administration Guide*.

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

The procedure for adding path-walk schedules is described in detail in the *Operations Manager Administration Guide*.

Note: Path walks can cause performance degradation. However, you can schedule your path walks to occur during low-use or nonbusiness hours.

Related references

[NetApp Host Agent configuration options](#) on page 33

NetApp Host Agent in a SAN

NetApp Host Agent resides on each SAN host that you want to monitor and enables you to monitor and manage SAN hosts through Operations Manager in a secure and platform-independent way.

Next topics

[NetApp Host Agent for SAN hosts](#) on page 23

[SAN terminology](#) on page 24

[Prerequisites for using NetApp Host Agent in a SAN](#) on page 24

[NetApp Host Agent information flow in a SAN](#) on page 25

NetApp Host Agent for SAN hosts

In a SAN environment, NetApp Host Agent is a network interface to HBA and LUN management utilities on a SAN host.

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. LUN management 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.

SAN terminology

Before configuring Operations Manager and NetApp Host Agent to monitor a SAN, familiarize yourself with these SAN terms and technologies.

Fiber Channel (FC)	Fiber 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, and 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 SAN to which SAN hosts send requests.
Initiator	An initiator is an HBA port on a SAN host that is used to initiate requests to a storage system in a SAN. Note: Initiator is also known as a host bus adapter or an HBA.
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.

Prerequisites for using NetApp Host Agent in a SAN

Before installing the NetApp Host Agent software, you should be familiar with setting up a NetApp SAN, as documented in the *Data ONTAP Block Access Management Guide for iSCSI and FC*.

Related information

Data ONTAP Block Access Management Guide for iSCSI and FCP -
http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml.

NetApp Host Agent information flow in a SAN

NetApp Host Agent obtains monitoring and management information about Windows hosts or on Solaris or Linux hosts.

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

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.

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 installation

The NetApp Host Agent software can be installed on Windows, Solaris, and Linux hosts.

Next topics

[NetApp Host Agent system requirements](#) on page 27

[Installing NetApp Host Agent](#) on page 29

[Uninstalling NetApp Host Agent](#) on page 30

NetApp Host Agent system requirements

NetApp Host Agent system requirements include supported platforms and compatible software versions.

For the complete list of supported devices, operating systems, and software versions, including those released after the production of this guide, see the "Support of NetApp Host Agent & SnapDrive for Windows" section of the DataFabric Manager Support Matrix on the NOW site at <http://now.netapp.com/>. Navigate to **Service and Support** ► **Technical Assistance and Documentation** ► **Access & Order Product Documentation**.

Next topics

[Operating systems that support NetApp Host Agent](#) on page 27

[Software versions that support NetApp Host Agent](#) on page 28

Operating systems that support NetApp Host Agent

You can install NetApp Host Agent on several different versions of Windows, Solaris, and Linux, as well as on VMware ESX server.

Platform	Supported operating system versions
Windows server	- Windows XP - Windows Server 2003 (32-bit and 64-bit) - Windows Vista - Windows 2008 Server (32-bit and 64-bit)
Solaris server	- Solaris 9 running on UltraSPARC - Solaris 10 running on UltraSPARC - Solaris 10 running on x86

Platform	Supported operating system versions
Linux workstation or server	- Red Hat Enterprise Linux ES v4 (Update 3 or later) on both 32-bit and 64-bit x86 - Red Hat Enterprise Linux AS v4 (Update 3 or later) on both 32-bit and 64-bit x86 - Red Hat Enterprise Linux Advanced Platform v5 on 32-bit and 64-bit x86 - SUSE Linux Enterprise Server 9, SP 2 or later (32-bit and 64-bit x86) - SUSE Linux Enterprise Server 10 (32-bit and 64-bit x86)
Oracle Enterprise Linux Support	- Oracle Enterprise Linux 4 (32-bit and 64-bit x86) - Oracle Enterprise Linux 5 (32-bit and 64-bit x86)
VMware ESX server, Standard or Enterprise Edition, version 3 and version 3.5	- Windows 2003 server (32 and 64-bit) - Windows XP, Windows Vista - Windows Server 2008 (32 and 64-bit) - Red Hat Enterprise Linux ES v4 (Update 3 or later) on both 32-bit and 64-bit x86 - Red Hat Enterprise Linux Advanced Platform v5 on both 32-bit and 64-bit x86 - Red Hat Enterprise Linux AS v4 (Update 3 or later) on both 32-bit and 64-bit x86 - Red Hat Enterprise Linux AS v5 (Update 3 or later) on both 32-bit and 64-bit x86 - SUSE Linux Enterprise Server 9 (SP2 or later) on 32-bit and 64-bit x86 - SLES 10 on both 32-bit and 64-bit x86

Software versions that support NetApp Host Agent

You can use NetApp Host Agent with several different versions of Operations Manager or SnapDrive for Windows.

NetApp Host Agent 2.7 supports the following software versions.

Software	Supported versions
Operations Manager	DataFabric Manager server 3.8 or later

Software	Supported versions
SnapDrive for Windows (to support SAN host monitoring)	SnapDrive for Windows 4.2, 4.2.1, 5.0, and 6.0

Note: For information about available software versions, see the DataFabric Manager Interoperability Matrix at <http://now.netapp.com/NOW/products/interoperability/>.

Installing NetApp Host Agent

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

Next topics

[Installing NetApp Host Agent from the NOW site](#) on page 29

[Installing NetApp Host Agent from a CD](#) on page 29

Installing NetApp Host Agent from the NOW site

You can download the NetApp Host Agent software from the NOW site .

Steps

1. Log in to the NOW site at <http://now.netapp.com/> .
2. Navigate to **Service and Support** ► **Software Download** ► **Download Software** ► **NetApp Host Agent**.
3. Select your platform and click **Go!**.
4. Follow the NOW site download and installation instructions.

Installing NetApp Host Agent from a CD

NetApp Host Agent is installed on third-party (Windows, Solaris, or Linux) hosts. You can install NetApp Host Agent from the DataFabric Manager CD.

Before you begin

Ensure that your host meets the system requirements.

Steps

1. Insert the CD into the CD-ROM drive of your Windows, Solaris, or Linux host.
2. Browse the CD; the installer files are located on the CD as described in the `index.htm` file.

3. Launch the installation file for your operating system.

If you are installing on a supported version of...	Then launch...
Windows	agentsetup-2-7-win32.exe
Solaris UltraSPARC	agentsetup-2-7-solaris.bin
Solaris x86	agentsetup-2-7-solaris-x86.bin
Linux	agentsetup-2-7-linux.bin

4. Follow the NetApp Host Agent setup prompts to complete the installation.

Uninstalling NetApp Host Agent

You can uninstall NetApp Host Agent from the command line or using the Windows Add/Remove programs utility.

Step

1. To uninstall NetApp Host Agent , complete the following step depending upon the platform from which you are removing it.

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

NetApp Host Agent administration

You can configure NetApp Host Agent to monitor SAN hosts through Operations Manager.

Next topics

- [Access to the user interface](#) on page 31
- [User privileges and security](#) on page 32
- [NetApp Host Agent passwords](#) on page 32
- [NetApp Host Agent configuration options](#) on page 33
- [Setting passwords in NetApp Host Agent](#) on page 34
- [Modifying settings for DataFabric Manager service](#) on page 35
- [Starting and stopping the NetApp Host Agent service](#) on page 35
- [Regenerating the host agent ID number](#) on page 36
- [The NetApp Host Agent log file](#) on page 37
- [Limitations of NetApp Host Agent](#) on page 37

Access to the user interface

The user interface to NetApp Host Agent is Web-based and you can access it from the computer on which NetApp Host Agent is installed or from any other computer on the network.

You can access the NetApp Host Agent user interface by HTTP or HTTPS. You can access configuration options or diagnostic information through HTTP or HTTPS. By default, NetApp Host Agent listens for HTTP requests on port 4092 and for HTTPS requests on port 4093.

In your Web browser, you must navigate to the appropriate URL, depending on whether you want to access configuration options or diagnostic information.

Type of access	URL
Configuration options	<code>http(s)://hostname(or IP address):port/admin</code> Following are examples of URLs that use IPv4 address: • <code>http://hostname:4092/admin</code> • <code>https://hostname:4093/admin</code> Following are the examples of URLs that use IPv6 address: • <code>http://[IPv6_address]:4092/admin</code> • <code>https://[IPv6_address]:4093/admin</code>

Diagnostic information	<code>http(s)://hostname(or IP address):port/about</code> Following are examples of URLs that use IPv4 address: • <code>http://hostname:4092/about</code> • <code>https://hostname:4093/about</code> Following are the examples of URLs that use IPv6 address: • <code>http://[IPv6_address]:4092/about</code> • <code>https://[IPv6_address]:4093/about</code>
------------------------	--

User privileges and security

NetApp Host Agent supports two levels of user privilege, both requiring password authentication.

User privilege levels

Monitoring privileges enable you to perform only monitoring functions.

Administration privileges enable you to perform both monitoring and administration functions.

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.

NetApp Host Agent 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

The DataFabric Manager server is configured to recognize the password `public` so that you can perform read-only operations 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.

Administration user name and password pair

The administration user name and password pair is as follows:

- User name = admin
- Password = *userspecified*

New installations of NetApp Host Agent disable management access until a password is configured for it. You specify the password using the host agent's configuration user interface. This user name and password pair allows read/write permission to the host agent. After setting the administration user name and password pair for 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

Password configuration in UNIX

Prior to NetApp Host Agent 2.5, UNIX users were required to have the root password and were unable to use the `sudo` option to configure passwords. In NetApp Host Agent 2.5 and later, the `-o` option lets you configure passwords without having root privileges. Here is example syntax that uses this option:

```
sudo ntap_agent -o Admin-Password=private
```

NetApp Host Agent configuration options

This table lists the configuration options, their functions, and the default values.

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 listens for HTTP requests	4092

Configuration option	Function	Default value
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
Filewalk Log path	Specifies the path for filewalk-related logs.	For Linux, <-> /opt/NTAPagent/filewalk For Windows, <-> C:\Program Files (x86)\NetApp\Agent\filewalk
DataFabric Manager server	Specifies the name of the DNS service with which the DataFabric Manager server is registered. Optionally, you can specify the IP address or host name of the DataFabric Manager server to which, NetApp Host Agent needs to be added voluntarily. Note: The DataFabric Manager server should have the network address of NetApp Host Agent configured.	datafabricmanager
DataFabric Manager port	Specifies the port number of the DataFabric Manager server.	8080

Setting passwords in NetApp Host Agent

You can change configuration options through the NetApp Host Agent Web-based user interface.

Before you begin

You must supply valid super user credentials on the host, to change configuration options in the NetApp Host Agent software. 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.

Steps

1. Access the NetApp Host Agent user interface from your browser.
2. At the login prompt, log in as the super-user.
3. If the NetApp Host Agent installation is new, configure the management password if it has not already been configured.
4. Change other options as needed.
5. Click **Update**.

Related concepts

[Access to the user interface](#) on page 31

Modifying settings for DataFabric Manager service

You can customize your DataFabric Manager server IP address and port number whose default values are "datafabricmanager" and "8080," respectively. The modification of these settings are for voluntary registration of host agents with DataFabric Manager server.

Steps

1. From the NetApp Host Agent **Welcome** page, click **Edit Settings**.
2. In the **Edit Settings** page, enter the IP address and port number.
3. Click **Update**.

Starting and stopping the NetApp Host Agent service

On Windows hosts, NetApp Host Agent runs as a service that starts automatically when the system boots up, and on Solaris or Linux hosts, NetApp Host Agent is a daemon started by the `init` service. You can start or stop the NetApp Host Agent service through the Windows services window or from the UNIX command line.

Before you begin

The NetApp Host Agent service must run with elevated permissions on some hosts:

- On Solaris and Linux hosts, the NetApp Host Agent daemon runs as root.

About this task

When NetApp Host Agent starts, it checks if another instance of NetApp Host Agent is running. If another instance is running, the second instance shuts down. No more than one instance can run at the same time.

Step

1. To start or stop the NetApp Host Agent service manually, perform the procedure for your type of host.

If your host is running...	Then...
Windows	Start and stop the NetApp Host Agent service through the Services window, as you would other Windows services.
Solaris or Linux	• To start the daemon, run the command <code>ntap_agent start</code>. • To stop the daemon, run the command <code>ntap_agent stop</code>.

Regenerating the host agent ID number

By deleting the existing host agent ID number, you can force NetApp Host Agent to generate a new host agent ID number when it restarts.

Steps

1. Stop the NetApp Host Agent service.
2. Delete the existing agent ID number using the procedure for your type of host.

If your host is running...	Then...
Windows	Delete the following registry value: <code>HKEY_LOCAL_MACHINE\SOFTWARE\NetApp\Agent\Config\System-ID</code>
Solaris or Linux	Remove the line that begins with <code>System-ID=</code> from the following configuration file: <code>/opt/NTAPagent/ntap_agent.cfg</code>

3. Restart the NetApp Host Agent service.

Related tasks

[Starting and stopping the NetApp Host Agent service](#) on page 35

The NetApp Host Agent log file

NetApp Host Agent maintains a single log file located in the installation directory.

Log file name and location

The log file is named `ntap_agent.log` and 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.

Limitations of NetApp Host Agent

Some limitations requiring workaround have been identified in the NetApp Host Agent software.

Next topics

[Discovery on cloned systems](#) on page 37

[Unresponsiveness with SnapDrive for Windows uninstall](#) on page 37

Discovery on cloned systems

DataFabric Manager cannot distinguish between "cloned" host agents.

NetApp Host Agent stores a unique system ID on each host on which it is installed. DataFabric Manager uses this ID to identify agents. When a system is "cloned," the ID number is copied and DataFabric Manager cannot distinguish between the two host agents. You can resolve this situation by forcing the agent to regenerate its ID number.

Related tasks

[Regenerating the host agent ID number](#) on page 36

Unresponsiveness with SnapDrive for Windows uninstall

NetApp Host Agent might not respond when installed along with SnapDrive for Windows on the same system.

In rare cases, NetApp Host Agent might not respond if you uninstall SnapDrive for Windows, but keep NetApp Host Agent installed. If you remove SnapDrive for Windows from the system, you must run the `ntap_agent start` command from the CLI, in the NetApp Host Agent install directory (by default, `C:\Program Files\NetApp\Agent`). This updates any service dependencies.

Index

A

- about NetApp Host Agent [13](#)
- API management password [33](#)
- API monitoring password [33](#)

C

- cloned systems [37](#)
- configuration
 - changing options [34](#)
 - options [33](#)

D

- DataFabric Manager service [35](#)

F

- flow of information in a SAN [25](#)
- FSRM
 - about [17](#)
 - capabilities [14](#)
 - configuration [21](#)
 - features [19](#)
 - license [19](#)
 - limitations [19](#)
 - management functions [17](#)
 - prerequisites [19](#)
 - storage space [18](#)
 - terminology [18](#)

H

- HTTP
 - port configuration [33](#)
- HTTPS
 - port configuration [33](#)
 - use [32](#)

I

- ID number
 - regenerating [36](#)
- installing NetApp Host Agent [29](#)
 - from CD [29](#)
 - from the NOW site [29](#)
- interface
 - user [31](#)
- IPv6 [13](#)

L

- license
 - FSRM [19](#)
- limitations [37](#)
- Linux
 - hardware requirements [27](#)
 - operating system requirements [27](#)
- log file
 - about [37](#)

M

- managing NetApp Host Agent [31](#)
- modify settings [35](#)

N

- NetApp Host Agent
 - starting and stopping [35](#)

O

- Operations Manager [13, 14](#)

P

- passwords
 - about [32](#)
 - administration [32](#)
 - API management [33](#)
 - API monitoring [33](#)

passwords (*continued*)

- configuration [32](#)
- DataFabric Manager server [20](#)
- Host Agent Management Password [20](#)
- Host Agent Monitoring Password [20](#)
- monitoring [32](#)
- security [32](#)

path [18](#)

path walk [18](#)

platform

- requirements [27](#)
- supported versions [27](#)

port information [31](#), [33](#)

prerequisites

- FSRM [19](#)
- SAN [24](#)

privileges

- user [32](#)

R

regenerating host agent ID number [36](#)

requirements

- credentials [34](#)
- DataFabric Manager [28](#)
- FSRM [19](#)
- Linux [27](#)
- operating system [27](#)
- Operations Manager [28](#)
- platform [27](#)
- SnapDrive for Windows [28](#)
- software [28](#)
- Solaris [27](#)
- system [27](#)
- Windows [27](#)

S

SAN

- capabilities [14](#)
- flow of information [25](#)
- prerequisites [24](#)
- with NetApp Host Agent [23](#)

security

- HTTPS [32](#)
- password [32](#)

software

- requirements [28](#)
- supported versions [28](#)

Solaris

- hardware requirements [27](#)
- operating system requirements [27](#)

system requirements [27](#)

T

terminology

- File Storage Resource Manager (FSRM) [13](#)
- FSRM [18](#)
- host agent [13](#)
- Microsoft Cluster Services (MSCS) [13](#)
- NetApp Host Agent [13](#)
- Operations Manager [13](#)
- SAN host [13](#)
- SnapDrive [13](#)

U

uninstalling [30](#)

unresponsiveness

- SnapDrive for Windows uninstall [37](#)

upgrade

- remote [33](#)

user interface

- about [31](#)
- ports used [31](#)

user privileges [32](#)

W

what NetApp Host Agent does [14](#)

Windows

- hardware requirements [27](#)
- operating system requirements [27](#)