

Foglight® for Storage Management 4.6
Installation Guide



© 2018 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (<https://www.quest.com>) for regional and international office information.

Patents


Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.


Trademarks


Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. "Apache HTTP Server", Apache, "Apache Tomcat" and "Tomcat" are trademarks of the Apache Software Foundation. Google is a registered trademark of Google Inc. Android, Chrome, Google Play, and Nexus are trademarks of Google Inc. Red Hat, JBoss, the JBoss logo, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries. CentOS is a trademark of Red Hat, Inc. in the U.S. and other countries. Fedora and the Infinity design logo are trademarks of Red Hat, Inc. Microsoft, .NET, Active Directory, Internet Explorer, Hyper-V, Office 365, SharePoint, Silverlight, SQL Server, Visual Basic, Windows, Windows Vista and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. AIX, IBM, PowerPC, PowerVM, and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Java, Oracle, Oracle Solaris, PeopleSoft, Siebel, Sun, WebLogic, and ZFS are trademarks or registered trademarks of Oracle and/or its affiliates in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries. Products bearing the SPARC trademarks are based on an architecture developed by Oracle Corporation. OpenLDAP is a registered trademark of the OpenLDAP Foundation. HP is a registered trademark that belongs to Hewlett-Packard Development Company, L.P. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries. Novell and eDirectory are registered trademarks of Novell, Inc., in the United States and other countries. VMware, ESX, ESXi, vSphere, vCenter, vMotion, and vCloud Director are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Sybase is a registered trademark of Sybase, Inc. The X Window System and UNIX are registered trademarks of The Open Group. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. "Eclipse", "Eclipse Foundation Member", "EclipseCon", "Eclipse Summit", "Built on Eclipse", "Eclipse Ready" "Eclipse Incubation", and "Eclipse Proposals" are trademarks of Eclipse Foundation, Inc. IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Apple, iPad, iPhone, Mac OS, Safari, Swift, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Ubuntu is a registered trademark of Canonical Ltd. Symantec and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. OpenSUSE, SUSE, and YAST are registered trademarks of SUSE LCC in the United States and other countries. Citrix, AppFlow, NetScaler, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. AlertSite and DéjàClick are either trademarks or registered trademarks of Boca Internet Technologies, Inc. Samsung, Galaxy S, and Galaxy Note are registered trademarks of Samsung Electronics America, Inc. and/or its related entities. MOTOROLA is a registered trademark of Motorola Trademark Holdings, LLC. The Trademark BlackBerry Bold is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Quest is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited. Ixia and the Ixia four-petal logo are registered trademarks or trademarks of Ixia. Opera, Opera Mini, and the O logo are trademarks of Opera Software ASA. Tevron, the Tevron logo, and CitraTest are registered trademarks of Tevron, LLC. PostgreSQL is a registered trademark of the PostgreSQL Global Development Group. MariaDB is a trademark or registered trademark of MariaDB Corporation Ab in the European Union and United States of America and/or other countries. Vormetric is a registered trademark of Vormetric, Inc. Intel, Itanium, Pentium, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Debian is a registered trademark of Software in the Public Interest, Inc. OpenStack is a trademark of the OpenStack Foundation. Amazon Web Services, the "Powered by Amazon Web Services" logo, and "Amazon RDS" are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries. Infobright, Infobright Community Edition and Infobright Enterprise Edition are trademarks of Infobright Inc. POLYCOM®, RealPresence® Collaboration Server, and RMX® are registered trademarks of Polycom, Inc. All other trademarks and registered trademarks are property of their respective

owners.

Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

-  **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Foglight for Storage Management Installation Guide
Updated - July 2018
Software Version - 4.6

Contents

Getting Started	7
Introducing the Storage Monitoring Architecture	7
Foglight for Storage Management Components	8
Network Ports Used	8
Sizing Your Monitored Environment	9
Ensuring System Requirements are Met	9
Small Environment System Requirements	10
Large Environment System Requirements	10
Requirements for Agent Managers	11
Installing or Enabling Foglight for Storage Management	12
Installing Foglight for Storage Management	12
Enabling Foglight for Storage Management from Foglight for Virtualization EE	13
Installed Dashboards and Cartridges	13
Adding a Full License	14
Renewing an Expired License	15
Configuring Agent Managers for Storage Collection	16
Installing External Agent Managers	16
Creating a Lockbox for Foglight for Storage Management Credentials	16
Supporting an Environment with Separate Fabrics that have Duplicated WWNs	16
Configuring Storage Collector Agents	17
Configuring VMware Performance Agents	18
Configuring Hyper-V Agents	18
Assigning Foglight for Storage Management Roles	18
Next Steps	19
Configuring Agents to Monitor Storage Devices	20
Brocade SAN Switches	20
Requirements for Brocade SAN Switches	21
Configuring Agents to Monitor Brocade SAN Switches	21
Cisco SAN Switches	22
Requirements for Cisco SAN Switches	22
Ensuring that SSH is Enabled on Switches	22
Configuring Agents to Monitor Cisco SAN Switches	23
Dell Compellent Arrays	23
Requirements for Dell Compellent Arrays	23
Configuring Agents to Monitor Dell Compellent Arrays	23
Dell EqualLogic PS Series Array Groups	24
Requirements for Dell EqualLogic Arrays	24
Configuring Agents to Monitor Dell EqualLogic Arrays	24
EMC CLARiiON CX Series Arrays (CLI)	24
Requirements for EMC CLARiiON CX Series Arrays (CLI)	25
Configuring Agents to Monitor EMC CLARiiON CX Series Arrays (CLI)	25
EMC CLARiiON, VNX, or VMAX Storage Arrays (SMI-S)	25

Requirements for EMC CLARiiON or VNX Arrays (SMI-S)	26
Requirements for EMC VMAX Arrays (SMI-S)	26
Configuring Agents to Monitor EMC Storage Arrays (SMI-S)	26
Configuring the SMI-S Provider for EMC CLARiiON or VNX	26
Verifying Statistics Logging is Enabled on EMC Arrays	29
EMC Isilon	31
Requirements for EMC Isilon	31
Configuring Agents to Monitor EMC Isilon Arrays	31
EMC VPLEX	31
Requirements for EMC VPLEX	32
Configuring Agents to Monitor EMC VPLEX Arrays	32
Hitachi Data Systems AMS, USP, and VSP	32
Requirements for Hitachi Data Systems AMS, USP, VSP	33
Configuring Agents to Monitor Hitachi Data Systems AMS	33
Configuring Agents to Monitor Hitachi Data Systems USP and VSP Arrays	33
HP EVA Storage Arrays	34
Requirements for HP EVA Storage Arrays	34
Configuring Agents to Monitor HP EVA Storage Arrays	34
HP 3PAR Arrays	34
Requirements for HP 3PAR Arrays	34
Enabling the SMI-S Provider	35
Configuring Agents to Monitor HP 3PAR Arrays	35
NetApp Filers	35
Requirements for NetApp Filers	35
Configuring Agents to Monitor NetApp Filers	38
Collection Target Support Matrix	38
Configuration Procedures	39
Configuring Agents to Monitor Storage Devices	40
Assigning Credentials	41
Resolving Connection Attempt Errors	42
Configuring the Hitachi Tuning Manager	43
Configuring Generic SMI-S Array Agent to Monitor Storage Devices	43
Managing Agents	45
Reviewing the Status of Configured Storage Collector Agents	45
Reviewing Agent Alarms	45
Editing Configured Agents	46
Reviewing Agent Status and Validating Connectivity	47
Managing Credentials	49
Managing Discovered Switches and Arrays	51
Managing CLARiiON Domains and Arrays	53
Managing the Hitachi Tuning Manager	53
Deploying Storage Agents after an Upgrade	55
About Us	56
We are more than just a name	56
Our brand, our vision. Together.	56

Contacting Quest	56
Technical support resources	56

Getting Started

The Getting Started workflow introduces you to Foglight for Storage Management, leads you through determining the system requirements that match the size of the monitored environment, and then walks through the steps to install and configure Foglight for Storage Management.

This workflow has the following steps:

- 1 [Introducing the Storage Monitoring Architecture](#)
- 2 [Sizing Your Monitored Environment](#)
- 3 [Ensuring System Requirements are Met](#)
- 4 [Installing or Enabling Foglight for Storage Management](#)
- 5 [Configuring Agent Managers for Storage Collection](#)
- 6 [Supporting an Environment with Separate Fabrics that have Duplicated WWNs](#)
- 7 [Configuring Storage Collector Agents](#)
- 8 [Configuring VMware Performance Agents](#)
- 9 [Configuring Hyper-V Agents](#)
- 10 [Assigning Foglight for Storage Management Roles](#)
- 11 [Next Steps](#)

Introducing the Storage Monitoring Architecture

Foglight for Storage Management provides complete monitoring of virtual storage environments, providing performance and capacity management metrics. It is designed for customers requiring storage monitoring functionality, but not full-fledged virtualization environment monitoring functionality.

Foglight for Storage Management monitors virtual environments, providing performance and capacity management metrics to assist you in:

- Improving management of virtual environments from host to storage.
- Gaining the information required to optimize storage performance associated with your virtual server environment.
- Ensuring service level agreements are met.
- Maintaining high levels of customer satisfaction.
- Avoiding the loss of cost savings already achieved with virtualization.

Foglight for Storage Management gathers extensive performance metrics and presents that data in a graphical interface using architectural diagrams, graphs, alerts, and drill-down screens to quickly identify virtual and physical storage problems. It fully supports VMware (vCenter and vSphere) and Hyper-V environments, allowing you to browse through your virtual infrastructure to identify storage performance, capacity, or topology issues.

Foglight for Storage Management Components

The following sections describe the components that make up Foglight for Storage Management.

Foglight for Storage Management

Foglight for Storage Management is built on Foglight, which provides the following components:

- **Management Server** — The Management Server receives information from agents, stores and processes data, and makes it available in the browser interface.
- **Agent Manager** — The Agent Manager is a middleware application that hosts agents, manages agent lifecycle (such as start, stop, and restart), manages the connection to the Management Server, and provides centralized services to agents.
- **Database Repository** — The database where data from all sources is collected and aggregated for display in the browser interface.
- **Browser Interface** — The interface you use to view data collected from your monitored environment and to investigate issues. You also use it to configure Foglight for Storage Management and perform administrative tasks.

For more information, see “Components” in the *Foglight for Storage Management Getting Started* online help.

Storage Collector Agent

Storage Collector Agents collect raw data from storage devices. You need to configure a Storage Collector Agent for each storage device you want to monitor.

Network Ports Used

Foglight for Storage Management uses several standard TCP/IP ports for its collections. These ports must be opened and traffic allowed between the storage devices and the Agent Manager hosts. The following table provides network port requirements by storage device.

Table 1. Network Port Requirements

Storage Device	Ports Used	Description
Brocade	5988 (non-SSL) 5989 (SSL)	SMI-S query to the management host
Cisco	22	SSH connection
Dell Compellent	3033	API to the host running Compellent Enterprise Manager
Dell EqualLogic	161	SNMP query to the EqualLogic Group Manager
EMC CLARiiON (CLI) on Unix	22	CLI-Navisphere connection to the management host using SSH
EMC CLARiiON (CLI) Windows	135 445 all ports above 1000	CLI-Navisphere connection to the management host using WMI (RPC)
EMC CLARiiON, VNX, VMAX (SMI-S)	5988 (non-SSL) 5989 (SSL)	SMI-S query to the host running the SMI-S Provider.
EMC Isilon	22	SSH connection using CLI

Table 1. Network Port Requirements

Storage Device	Ports Used	Description
Hitachi Data Systems	5988 (non-SSL)	SMI-S query to the host running the Hitachi Command Suite or embedded SMI-S provider on VSP arrays.
	5989 (SSL)	
	Tuning Manager uses:	When running the Tuning Manager, the connection to the management host uses WMI (RPC).
	135	
	445	
	all ports above 1000	
HP EVA	5988 (non-SSL)	SMI-S query to the host running Command View
	5989 (SSL)	
NetApp	80	DataOnTap API query to each filer
	443	
3PAR	5988 (non-SSL)	SMI-S query to an embedded SMI-S provider on the array.
	5989 (SSL)	

Sizing Your Monitored Environment

IMPORTANT: You should not consider a production implementation without first conducting a proper scoping and sizing exercise. To arrange for a sizing analysis, contact your Quest Software Sales representative.

The number of physical disks (among all monitored storage arrays and filers) in the monitored environment is a rough guide to the size of the Foglight for Storage Management collection environment.

Table 2. Physical disks and system requirements

Number of VMs	System Requirements
Fewer than 2000 disks	See Small Environment System Requirements
More than 2000 disks	See Large Environment System Requirements

Ensuring System Requirements are Met

Due to the potential for a very large number of objects being collected, analyzed, and maintained by the application, there are several aspects of the underlying server that must be taken into account. The sizing of the supporting server or virtual machine (VM), depends upon the size and complexity of the underlying environment.

Sufficient processing power and CPU memory must be present to support effective collection and server data handling and analytics. Collected data is staged in memory prior to passing to the collector database.

The following sections describe the requirements for small and large collection environments, as well as for the Agent Manager.

- [Small Environment System Requirements](#)
- [Large Environment System Requirements](#)
- [Requirements for Agent Managers](#)

Small Environment System Requirements

A small collection environment can typically have its storage collection handled by using the StorageCollector agents installed on the embedded Agent Manager that is available on the Foglight Management Server machine. The resource requirements shown below are the minimum needed for collection in a small environment.

NOTE: If scalability is important, use an external Agent Manager instead of the embedded Agent Manager. Follow the system requirements described in [Large Environment System Requirements](#) instead of these requirements.

Foglight for Storage Management (all components) on a 64-bit Windows or Linux Platform

Table 3. System Requirements

CPU	8-way 2.4 GHz CPUs — one of the following: <ul style="list-style-type: none">• 2 quad core• 4 dual core• 8 single core
RAM	20 GB in total: <ul style="list-style-type: none">• 10 GB for the Management Server• 6 GB for the Management Server Database Repository• 2 GB for the operating system• 2 GB for Agent Managers and agents and repository
Storage	Storage: <ul style="list-style-type: none">• 20 GB for the Management Server• 100 GB for the Management Server Database Repository If using an embedded database repository: <ul style="list-style-type: none">• Total of 140 GB on a RAID device available on the Management Server machine If using an external Database Repository: <ul style="list-style-type: none">• 40 GB on a RAID device available on the Management Server machine• 100 GB on a RAID device for the external Database Repository

Databases must be regularly backed up and maintained to reduce wasted space.

Large Environment System Requirements

A large collection environment requires that the Agent Manager for the Storage Collector agents be installed on a server that is separate from the server running the Management Server. Requirements for both machines are outlined below. Refer to the System Requirements and Platform Support Guide for virtual machine and Agent Manager collection requirements.

Table 4. Management Server, Browser Interface, and Database Repository on a 64-bit Foglight-supported Platform

	4-way 2.4 GHz CPUs — one of the following:
CPU	<ul style="list-style-type: none"> • 1 quad core • 2 dual core • 4 single core
	28 GB in total:
RAM	<ul style="list-style-type: none"> • 16 GB for the Management Server • 8 GB for the Database Repository • 4 GB for the operating system
	If using a built-in embedded Database Repository:
	<ul style="list-style-type: none"> • 220 GB, on a RAID device
Storage	If using an external Database Repository:
	<ul style="list-style-type: none"> • For Management Server: 60 GB, on a RAID device • For Database Repository: 160 GB, on a RAID device

Table 5. Agent Manager on a 64-bit Windows or Linux Platform

	4-way 2.4 GHz CPUs — one of the following:
CPU	<ul style="list-style-type: none"> • 1 quad core • 2 dual core • 4 single core
	6 GB in total:
RAM	<ul style="list-style-type: none"> • 5 GB for Agent Manager and agents • 1 GB for operating system
Storage	30 GB on a RAID device

Databases must be regularly backed up and maintained to reduce wasted space.

Requirements for Agent Managers

Whether you use the embedded Agent Manager or external Agent Managers, you need to make sure that the hosting server meets the supported platform requirements. Agent Managers that are used for Foglight for Storage Management collections must be installed on a server running a supported 64-bit Linux operating system or a supported 64-bit Microsoft Windows operating system.

Foglight for Storage Management has been tested on the following environments.

Table 6. Test Environments

Operating System	Version	OS Architecture	Valid Installer
CentOS® Linux®	7.x	x86-64	<i>fglam-<ver>-linux-x86_64.bin</i>
Microsoft® Windows®	Server 2008	x86-64	<i>fglam-<ver>-windows-x86_64.exe</i>
	Server 2008RS	x86-64	<i>fglam-<ver>-windows-x86_64.exe</i>
	Server 2012		
	Server 2012 R2		
Novell® SUSE Linux® Enterprise Server	11	x86-64	<i>fglam-<ver>-linux-x86_64.bin</i>

Table 6. Test Environments

Operating System	Version	OS Architecture	Valid Installer
Red Hat® Enterprise Linux®	6.x	x86-64	<i>fglam-<ver>-linux-x86_64.bin</i>
Ubuntu® Linux	14.04.x LTS	x86-64	<i>fglam-<ver>-linux-x86_64.bin</i>

Installing or Enabling Foglight for Storage Management

Your next step depends on whether you already have Foglight for Virtualization, Enterprise Edition (Foglight for Virtualization EE) installed.

- If Foglight for Virtualization EE is not installed, see [Installing Foglight for Storage Management](#).
- If Foglight for Virtualization EE is installed, see [Enabling Foglight for Storage Management from Foglight for Virtualization EE](#).

Both options provide a trial license for Foglight for Storage Management.

This section covers the following topics:

- [Installing Foglight for Storage Management](#)
- [Enabling Foglight for Storage Management from Foglight for Virtualization EE](#)
- [Installed Dashboards and Cartridges](#)
- [Adding a Full License](#)
- [Renewing an Expired License](#)

Installing Foglight for Storage Management

At the end of this procedure, Foglight for Storage Management is installed with a trial license enabled.

i | **TIP:** The installer also installs the components for Foglight for Virtualization EE, so if you are interested in extending your monitoring capabilities to your entire virtualized environment, you can enable a trial license for Foglight for Virtualization EE from within the product.

To install Foglight for Storage Management:

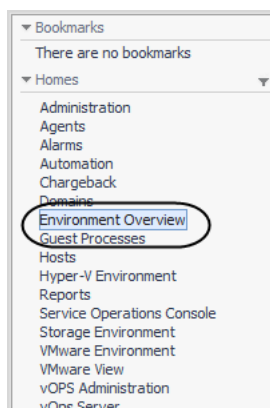
- 1 Start the installation wizard by initiating the executable included on the Foglight for Storage Management installation media.
- 2 Follow the online instructions. You need to accept the terms of the license agreement to install this product.
- 3 When the installation is complete, click **Done**.
The Foglight for Storage Management login page appears.
- 4 Enter a valid username and password and click **Login**.
Foglight for Storage Management opens to the Storage Environment dashboard.

Enabling Foglight for Storage Management from Foglight for Virtualization EE

You already have the components for Foglight for Storage Management installed; all you need to do is enable the trial license.

To enable Foglight for Storage Management from Foglight for Virtualization EE:

- 1 Log in to Foglight for Virtualization, Enterprise Edition.
- 2 On the navigation panel, under **Homes**, choose **Environment Overview**.



- 3 Click the Foglight for Storage Management **Start Trial** button.
The Foglight for Storage Management trial license is enabled.

Installed Dashboards and Cartridges

Foglight for Storage Management adds a set of storage-specific dashboards to the core Foglight for Storage Management components.

Dashboards

Storage-specific dashboards are located under **Storage & SAN** in the navigation panel:

- **Storage Capacity** — Monitor your storage capacity by device type.
- **Storage Environment** — Configure the monitored storage environment, monitor and investigate storage devices, and maintain the solution.
- **Storage Explorer** — Investigate issues in storage performance.
- **Storage Troubleshooting** — Determine if a poorly-performing virtual machine is experiencing storage issues.

Storage information can also be found in the following menus/dashboards:

- **VMware or Hyper-V Explorer** — Review the entities that make up the virtual environment, from vCenters to datastores or servers. The VMware Explorer and Hyper-V Explorer ships with both Foglight for Virtualization Enterprise Edition and Foglight for Storage Management. When adding Foglight for Storage Management to Foglight for Virtualization EE, you gain the ability to view connectivity diagrams that link datastores to the SAN environment in the following tabs:
 - **SAN Topology tab** — View a diagram showing how the selected entity connects to the storage environment. Click an icon or name to drill down the component dashboard. This tab is available on the following dashboards: Cluster, Datastore, ESX Host, Hyper-V server, and Virtual Machine.

- **SAN Data Path tab** — View a table and a diagram containing performance metrics for the ports providing I/O to and from storage devices and their components. Click an icon or name to drill down the component dashboard. This tab is available on the following dashboards: ESX Host, Hyper-V server, and Virtual Machine.
- **Infrastructure** — Review the physical hosts that underlie the virtual environment. The Infrastructure Environment dashboard ships with both Foglight for Virtualization Enterprise Edition and Foglight for Storage Management. When adding Foglight for Storage Management to Foglight for Virtualization EE, you gain the ability to infer the name of physical hosts that are connected to storage devices *without* having to create Infrastructure agents to monitor physical hosts directly. These hosts are referred to as *Inferred Hosts*.

Cartridges

The storage-specific functionality is packaged in one car containing the following cartridges:

- Storage
- Storage Collector
- Storage-Intelliprofile
- StorageUI

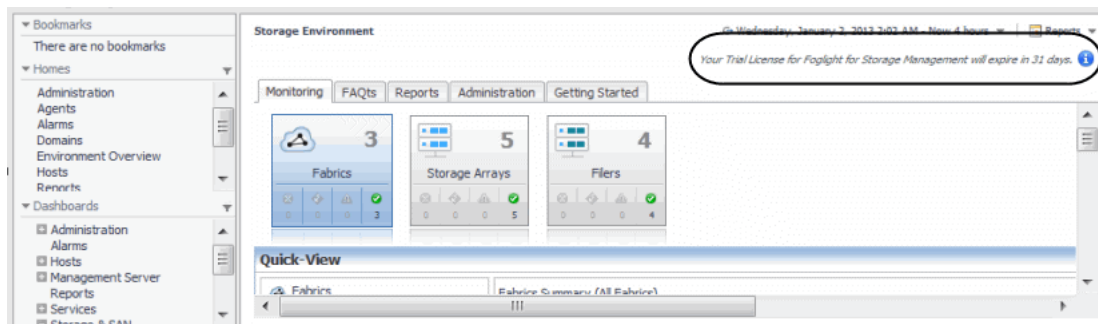
To view the status of installed cartridges, on the navigation panel, under Dashboards, click **Administration > Cartridges > Cartridge Inventory**. Scroll down to find the cartridges.

Adding a Full License

The Foglight for Storage Management license status appears below the date and time range under the following circumstances:

- A trial license is installed.
- A term license is within 30 days of expiration.
- A license has expired.

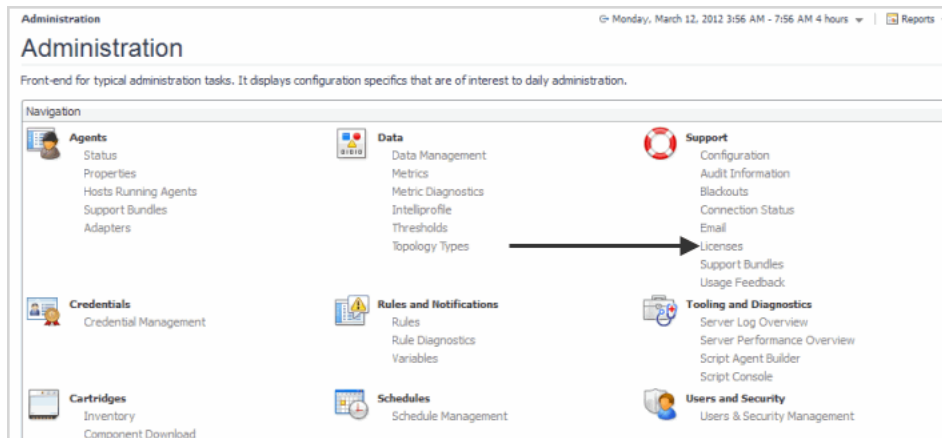
Figure 1. License status



If you want to upgrade from a trial license to a full license, or replace an expiring license, contact a Quest Software Sales representative to purchase a license.

To install a full license:

- 1 Log in to Foglight for Storage Management.
- 2 On the navigation panel, under **Homes**, click **Administration**.
- 3 On the Administration dashboard, under Support, click **Licenses**.



- 4 On the Manage Licenses dashboard, click **Install**.
The Install License dialog box opens.
- 5 Click **Browse**.
- 6 Navigate to and select the license.
- 7 Click **Open**.
- 8 Click **Install License**.
The license is installed and is displayed in the licenses table.

Renewing an Expired License

When the Foglight for Storage Management license is expired, a warning message is displayed in the Storage Environment dashboard > Administration tab.

To install a new license:

- 1 Open the Storage Environment dashboard > Administration tab.
If the license is expired, the tab displays a warning message (“Your Foglight Storage Manager License is Expired”).
- 2 Click the **Click to Install License** button at the bottom of the view.
The new license is installed. When the operation completes, the Administration tab is updated to display information about what you need to do after installing a new license (“You need to enable the Storage Collector Cartridge”).
- 3 In the How to re-enable Storage Monitoring section > Step 2, click the **Click here** link to view the list of installed cartridges.
- 4 Navigate to Dashboards > Administrations > Cartridges > Cartridge Inventory.
- 5 In the Installed Cartridge tab, locate the **StorageCollector** cartridge, select its checkbox, and click **Enable** at the top of the table.
- 6 Ensure that all storage agents are active and collecting data.

Configuring Agent Managers for Storage Collection

If you are installing external Agent Managers, install them now and then return to this workflow to configure some settings for storage collection.

This section covers the following topics:

- [Installing External Agent Managers](#)
- Optional — [Creating a Lockbox for Foglight for Storage Management Credentials](#)

Installing External Agent Managers

If you are installing external Agent Managers, first ensure that the servers that host the external Agent Managers meet the requirements listed under [Large Environment System Requirements](#) and [Requirements for Agent Managers](#). Then follow the instructions under “Installing external Agent Managers” in the *Foglight Agent Manager Guide*.

Creating a Lockbox for Foglight for Storage Management Credentials

Lockboxes enable you to store encrypted credentials in a central location and organize credentials into meaningful groups. A credential contains the user account information required to access a monitored device, such as a login name and password.

The Agent Manager has a default lockbox named *System*. You can use this lockbox, or you can create a separate lockbox to group the credentials used to access storage devices. If you want to create a lockbox, you should do it now, because when you begin configure Storage Collector Agents, the wizard prompts you to assign credentials in lockboxes.

To create a lockbox:

- 1 On the navigation panel, under Dashboards, click **Administration > Credentials**.
- 2 Click **Manage Credentials**.
- 3 Click **Add**.
- 4 Type a name such as **Storage** and optionally a password.
- 5 Click **Add**.

Supporting an Environment with Separate Fabrics that have Duplicated WWNs

Foglight for Storage Management uses WWNs as unique identifiers for mapping SAN topologies.

If you are using HP Virtual Connect capability, or another similar product, to allow fabrics in different datacenters to use the same WWN ranges in your SANs, additional steps must be taken to allow a single Foglight installation to process the collected data properly.

The **Storage & San > Storage Environment > Administration** dashboard provides a task called **Configure Duplicate WWN Support**. Click on this task to display a dialog that will let you specify prefix values that Foglight will prepend to collected WWN values to create unique identifiers within Foglight.

The datacenters with overlapping WWN ranges must be configured with different FglAMs for each datacenter.

All the FglAMs that collect from devices that interconnect must be configured to use the same prefix. Typically this would be all the FglAMs supporting a physical location or datacenter. These identifiers will apply to storage devices and virtualization devices.

Failure to provide unique identifiers in this situation will result in incorrect topology diagrams being displayed, and it may also cause performance problems.

Configuring Storage Collector Agents

In this step, you configure Storage Collector Agents to monitor supported storage devices. A wizard leads you through the process. Depending on the storage device, the details of the process may be different, but the general activities remain the same.

The general workflow follows these steps:

- 1 Ensure that the storage device meets Foglight for Storage Management requirements.
- 2 Launch the Storage Device Setup dialog.
- 3 Select the type of storage device to monitor.
- 4 Specify the IP address of the storage device and any other requested information.
- 5 Assign credentials for the storage device.
- 6 Release the Agent Manager lockbox (once per Agent Manager).
- 7 Complete other device-specific configuration.
- 8 Verify that the configured agent can connect to the storage device.

To begin configuring a Storage Collector Agent (hereafter referred to simply as agent), select the target storage device from the following list. For each device, the collection method is described first, followed by requirements, and then the configuration procedure.

- [Brocade SAN Switches](#)
- [Cisco SAN Switches](#)
- [Dell Compellent Arrays](#)
- [Dell EqualLogic PS Series Array Groups](#)
- [EMC CLARiiON CX Series Arrays \(CLI\)](#)
- [EMC CLARiiON, VNX, or VMAX Storage Arrays \(SMI-S\)](#)
- [EMC Isilon](#)
- [EMC VPLEX](#)
- [Hitachi Data Systems AMS, USP, and VSP](#)
- [HP EVA Storage Arrays](#)
- [HP 3PAR Arrays](#)
- [NetApp Filers](#)

If you later need to edit an agent configuration, see [Editing Configured Agents](#).

Configuring VMware Performance Agents

Foglight for Storage Management includes a license for the VMware-lite component, which is used for monitoring virtual machines running under VMware vSphere and vCenter. If you want full-fledged VM monitoring, you need to add a license for Foglight for Virtualization EE. For more information, see [Installing Foglight for Storage Management](#).

i | **IMPORTANT:** If you enabled Foglight for Storage Management from Foglight for Virtualization EE, you should already have VMware Performance agents monitoring your vCenters. Instead of completing this procedure, edit the agent and select Enable Storage Collection. If you need more information, see “Collecting Datastore-to-SAN Relationships” in the *Foglight for Storage Management User and Reference Guide*.

You need to configure a VMware Performance Agent for each vCenter you want to monitor. If you later need to edit an agent configuration, see [Editing Configured Agents](#).

For detailed information about how to create and configure a VMware Performance Agent to collect data from a vCenter®, see the topic “Configuring monitoring agents for data collection” in the *Foglight for VMware User and Reference Guide*.

Configuring Hyper-V Agents

Foglight® for Storage Management uses the Hyper-V Agent to collect information from monitored hosts. Creating a Hyper-V Agent instance creates the agent process on the Agent Manager host. Activating the Hyper-V Agent starts that agent process while starting an agent instance’s data collection enables the agent to start collecting data from the monitored host and to send it to Foglight for Storage Management.

When the Hyper-V Agent package is successfully deployed, create one or more agent instances, activate them, and start their data collection. To perform these steps in a single operation for one or more monitored hosts, use the **Agents** area on the **Administration** tab of the Hyper-V Environment dashboard.

For detailed information about how to create, activate Hyper-V Agent instances, and start their data collection, see the topic “Configuring monitoring agents” in the *Foglight for Hyper-V User and Reference Guide* or *Hyper-V Monitoring in Foglight for Storage Management User and Reference Guide*, whichever applies.

Assigning Foglight for Storage Management Roles

Foglight for Storage Management adds the following Storage user roles to the Foglight for Storage Management roles.

Table 7. Storage user roles.

Roles	Description
Storage Administrator	<ul style="list-style-type: none"> Perform administrative tasks from the Storage Environment dashboard. <i>Excludes actions reserved for the Foglight for Storage Management Administrator role, such as creating and modifying agents, rules, and registry variables.</i> View all Storage & SAN dashboards. Create and manage Storage reports.
Storage QuickView User	<ul style="list-style-type: none"> View all Storage & SAN dashboards. Create and manage Storage reports.
Storage Report User	<ul style="list-style-type: none"> View Storage reports only.

When creating user accounts that include one of the Storage user roles, you also need to assign the following group and roles to support the desired features:

- **Foglight for Storage Management Operators group** — *Required* — Assign this group to all Foglight for Storage Management users to enable access to the Foglight for Storage Management console.
- **General Access role** — *Required* — Assign this role to all Foglight for Storage Management users to enable the Foglight for Storage Management reporting features that support Storage reports.
- **VMware Administrator and Hyper-V Administrator role** — *Recommended* — Assign this role to *Storage Administrators* and *Storage QuickView Users* unless you specifically want to prohibit a user from seeing and using the VMware or Hyper-V menus and dashboards.
- **Administrator role** — When appropriate, assign this role to the *Storage Administrators* who should also have permission to create and modify agents, rules, and registry variables.

i | **NOTE:** To create and manage user accounts, your user account must have the group Foglight Administrators assigned. This group includes the Administrator role as well as the necessary roles to enable unrestricted access to all Foglight tasks and dashboards.

To begin, navigate to the **Administration > Users & Security** dashboard. For instructions, open the online help and click **More**.

Next Steps

For each of your users, provide them with their user credentials and the IP address of the Foglight for Storage Management browser interface where they can log in to Foglight for Storage Management. Storage users can immediately begin monitoring the storage environment and investigating issues. For help on these tasks, and for information about modifying data collection and alarm settings, see the Foglight for Storage Management User and Reference Guide.

For agent and agent manager maintenance, backup tasks, troubleshooting, and upgrade information, see [Managing Agents](#).

Configuring Agents to Monitor Storage Devices

This section contains the supported storage devices by vendor, requirements for each device, and procedures to help you complete the screens in the Storage Device Setup dialog box.

This section includes the following topics:

- [Brocade SAN Switches](#)
- [Cisco SAN Switches](#)
- [Dell Compellent Arrays](#)
- [Dell EqualLogic PS Series Array Groups](#)
- [EMC CLARiON CX Series Arrays \(CLI\)](#)
- [EMC CLARiON, VNX, or VMAX Storage Arrays \(SMI-S\)](#)
- [EMC Isilon](#)
- [EMC VPLEX](#)
- [Hitachi Data Systems AMS, USP, and VSP](#)
- [HP EVA Storage Arrays](#)
- [HP 3PAR Arrays](#)
- [NetApp Filers](#)
- [Configuration Procedures](#)

Brocade SAN Switches

Foglight for Storage Management uses the SMI-S interface to collect from Brocade SAN switches.

Brocade switch information is collected using the following namespaces:

- **Interop Namespace** — `interop`
- **Working Namespace(Brocade)** — `root/brocade1`
- **Working Namespace(McData)** — `root/mcdata`

Foglight for Storage Management executes the following SMI-S commands to obtain switch information on all SAN switches or Switch Management applications:

- `EnumerateInstanceNames`
- `EnumerateInstances`
- `References`
- `Reference Names`
- `Associators`

- Associator Names
- GetClass

For more information, see the following topics:

- [Requirements for Brocade SAN Switches](#)
- [Configuring Agents to Monitor Brocade SAN Switches](#)

Requirements for Brocade SAN Switches

Requirements differ depending on the version of Brocade Fabric OS (FOS) used by your switch.

Brocade Switches on FOS 7.0 or later

For Brocade switches running FOS 7.0 or later, Foglight for Storage Management collects information from the switches using the Brocade Network Advisor (BNA). Foglight for Storage Management works with either the full commercial version of BNA (license required) or the SMI-S only version of BNA (free).

Your environment must meet the following requirements:

- Brocade Network Advisor is installed, either the full version or the free SMI-S Only mode version.
- Brocade switches are *not* configured as Access Gateway switches. Foglight for Storage Management does not collect from switches configured as Access Gateway switches.
- Foglight for Storage Management requires a user account with read access. An account with write/admin access is required to add the switch to BNA, but is not required for monitoring.

Brocade Switches on earlier versions of FOS

Foglight for Storage Management collects information from Brocade switches on earlier versions of FOS via a Brocade SMI Agent on a management host. The SMI Agent talks to proxy switches, one in each fabric. These proxy switches are identified through the use of a configuration tool provided by the SMI Agent. Foglight for Storage Management does not perform any configuration of the SMI Agent. The account is native to the SMI Agent.

For information on acquiring, installing, and setting up the Brocade SMI Agent, see: <http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page>

Your environment must meet the following requirements:

- The Brocade SMI server is installed on a server/host other than the server/host running the Foglight for Storage Management Agent Manager.
- The SMI Agent is enabled (it is not enabled by default).
- The SMI Agent requires a CIMOM that is SMI-S 1.1 or 1.2 CTP conformant.
- Brocade switches are *not* configured as Access Gateway switches. Foglight for Storage Management does not collect from switches configured as Access Gateway switches.
- Foglight for Storage Management requires a user account with read access. An account with write/admin access is required to add the switch to BNA, but is not required for monitoring.

Configuring Agents to Monitor Brocade SAN Switches

You configure an agent to monitor the Brocade management server hosting the SMI Agent. All switches managed by this management server are monitored. For details, see [Configuring Agents to Monitor Storage Devices](#).

Cisco SAN Switches

Foglight for Storage Management collects information from Cisco switches through the native MDS 9000 - 9700 series embedded SAN/NX-OS System software CLI.

For more information, see the following topics:

- [Requirements for Cisco SAN Switches](#)
- [Ensuring that SSH is Enabled on Switches](#)
- [Configuring Agents to Monitor Cisco SAN Switches](#)

Requirements for Cisco SAN Switches

Your environment must meet the following requirements:

- Each Cisco switch has a valid SSH interface.
- Foglight for Storage Management requires a valid user account with read/write access on each Cisco switch in the SAN. The CLI command types used are:

```
show hardware
show wwn switch
show flogi database
show interface | include "fc|Port mode|Port WWN"
show interface | include "fc|Port WWN"
show interface counters
show vsan
```

Ensuring that SSH is Enabled on Switches

Log in to the switch and check that SSH is enabled.

To check that SSH is enabled on the switch:

- 1 Log in to the switch using Telnet.
- 2 At the command line, enter the following (the command entered is in bold):

```
switch-name# show ssh server
```

The response will be either:

```
ssh is not enabled
```

```
ssh is enabled
```

- 3 If SSH is not enabled, complete the following steps:
 - a Enter the following command:

```
switch-name# config t
```
 - b Enter the following configuration commands, one per line:

```
switch-name(config)# enable ssh server
switch-name(config)# exit
```
 - c Verify that SSH is enabled by entering the following command:

```
switch-name# show ssh server
```

The response should be:

```
ssh is enabled
```

```
Version 2 is enabled
```

4 Type **Ctrl/Z**.

Configuring Agents to Monitor Cisco SAN Switches

During this procedure you create an agent for a Cisco switch. The dialog allows you to create multiple agents for other switches that use the same credentials. For switches in the same Fabric, you need to configure agents to use the same Agent Manager.

For details, see [Configuring Agents to Monitor Storage Devices](#).

Dell Compellent Arrays

Foglight for Storage Management collects information from Dell Compellent arrays using an API provided by Dell Storage Manager or Compellent Enterprise Manager software. A single agent can collect from all the arrays visible in Dell Storage Manager or Enterprise Manager.

For more information, see the following topics:

- [Requirements for Dell Compellent Arrays](#)
- [Configuring Agents to Monitor Dell Compellent Arrays](#)

Requirements for Dell Compellent Arrays

Your environment must meet the following requirements:

- For supported Dell Storage Manager or Compellent Enterprise Manager, see [Collection Target Support Matrix](#).
- Foglight for Storage Management requires a valid Storage Manager or Enterprise Manager user account. Use the Dell Storage Manager or Enterprise Manager Data Collector Manager to configure a user account with Administrator privileges.
- Storage Manager or Enterprise Manager requires an account with administrative access to add a Compellent Array and to communicate with the array.

Configuring Agents to Monitor Dell Compellent Arrays

In this procedure, you configure the agent to monitor the Compellent Storage Manager or Enterprise Manager host, then you select the arrays to monitor. For details, see [Configuring Agents to Monitor Storage Devices](#).

Dell EqualLogic PS Series Array Groups

Foglight for Storage Management uses SNMP to collect information about Dell EqualLogic PS Series array groups. Foglight for Storage Management requires a separate agent for each Dell EqualLogic PS Series array group. The agent uses the array group's SNMP community name to collect and organize information about the groups. For more information, see the following topics:

- [Requirements for Dell EqualLogic Arrays](#)
- [Configuring Agents to Monitor Dell EqualLogic Arrays](#)

Requirements for Dell EqualLogic Arrays

Your environment must meet the following requirements:

- For supported PS Firmware, see [Collection Target Support Matrix](#).
- SNMP community names exist for each array group. You configure SNMP names using the EqualLogic Group Manager. For more information, see "Displaying and Configuring SNMP Access to a Group" in the EqualLogic Group Manager online help.

Configuring Agents to Monitor Dell EqualLogic Arrays

During this procedure you create an agent for an EqualLogic PS Series array group. The dialog allows you to create multiple agents for other array groups that use the same credentials.

For details, see [Configuring Agents to Monitor Storage Devices](#).

EMC CLARiiON CX Series Arrays (CLI)

Foglight for Storage Management uses the NaviSecCLI utility on the EMC Management Host to collect data from EMC CLARiiON CX Series arrays. When accessing specific CLARiiON arrays, Foglight for Storage Management uses the Navisphere management application (via the NaviSecCLI) for collection. Foglight for Storage Management requires an EMC Management Host user account to access Navisphere, as well as a Navisphere account to access the individual arrays.

i | **NOTE:** NaviSecCLI is not supported for monitoring EMC VNX or VMAX arrays. However, you can monitor these arrays using the SMI-S interface. For instructions, see [EMC CLARiiON, VNX, or VMAX Storage Arrays \(SMI-S\)](#).

For more information, see the following topics:

- [Requirements for EMC CLARiiON CX Series Arrays \(CLI\)](#)
- [Configuring Agents to Monitor EMC CLARiiON CX Series Arrays \(CLI\)](#)

Requirements for EMC CLARiiON CX Series Arrays (CLI)

Your environment must meet the following requirements:

- NaviSphere is running on a different server than the Foglight Agent Manager. This server is referred to as the EMC Management host.
- For supported NaviSphere CLI version, see [Collection Target Support Matrix](#).
- Statistics logging is enabled on each array. See [Verifying Statistics Logging is Enabled on EMC Arrays](#).
- Foglight for Storage Management requires the following accounts:
 - An EMC Management Host user account to access the NaviSphere NaviSecCLI utility, with the following access privileges:
 - On UNIX systems, SSH services with read and execute access to the binaries (sudo if the administrator changed the access privileges).
 - On Windows systems, read and execute access to the executables. In addition, the following shares and services are required to access Navisphere:
 - ADMIN\$, IPC\$ as Shares
 - RPC service enabled
 - A Navisphere account with the Global privilege. This account is used by the NaviSecCLI commands to access the individual arrays. The Global privilege provides access to all CLARiiON arrays in the Navisphere domain, requiring the user to provide the IP for only a single Service Processor (SP) of an array in the domain.

Configuring Agents to Monitor EMC CLARiiON CX Series Arrays (CLI)

During this procedure, you configure the agent to use the CLI to collect from the array management host. For details, see [Configuring Agents to Monitor Storage Devices](#).

EMC CLARiiON, VNX, or VMAX Storage Arrays (SMI-S)

To collect from EMC CLARiiON and VNX arrays, Foglight for Storage Management uses the EMC SMI-S Provider installed on a host machine. For EMC VMAX arrays, Foglight for Storage Management uses the EMC SMI-S Provider installed on EMC Solutions Enabler. The SMI-S Provider can be downloaded from the EMC Support page at <https://support.emc.com/downloads>.

For more information, see the following topics:

- [Requirements for EMC CLARiiON or VNX Arrays \(SMI-S\)](#)
- [Requirements for EMC VMAX Arrays \(SMI-S\)](#)
- [Configuring Agents to Monitor EMC Storage Arrays \(SMI-S\)](#)
- [Configuring the SMI-S Provider for EMC CLARiiON or VNX](#)
- [Verifying Statistics Logging is Enabled on EMC Arrays](#)

Requirements for EMC CLARiiON or VNX Arrays (SMI-S)

Your environment must meet the following requirements:

- For supported Solutions Enabler and SMI-S provider versions for each array model, see [Collection Target Support Matrix](#).
- Statistics logging is enabled on each array. See [Verifying Statistics Logging is Enabled on EMC Arrays](#).
- For compatibility information with EMC Solutions Enabler, CLARiiON Navisphere, and VNX Unisphere releases, see the *SMIS Provider Release Notes*.
- Foglight for Storage Management requires an SMI-S account with the Monitor role. For help setting up an Monitor account, see the *SMIS Provider Release Notes*.

i | **IMPORTANT:** EMC has deprecated some storage systems with the 8.0.1 release of Solutions Enabler. For more information refer to <https://support.emc.com/docu55547>. An EMC support account is required. As a result, customers wishing to monitor any VNX array or any CLARiiON CX, CX3, CX4, AX, AX4 series array must use a 7.6.x release of Solutions Enabler.

Requirements for EMC VMAX Arrays (SMI-S)

Your environment must meet the following requirements:

- For supported Solutions Enabler and SMI-S provider versions for each VMAX array, see [Collection Target Support Matrix](#). Contact EMC Customer Service to enable SMI-S Provider on the service processor. EMC requires involving EMC Customer Service when starting and stopping Solutions Enabler services and the SMI-S Provider.
- Foglight for Storage Management requires an SMI-S account with the Monitor role. For help setting up a monitor account, see the *SMIS Provider Release Notes*.

i | **IMPORTANT:** EMC has deprecated some storage systems with the 8.0.1 release of Solutions Enabler. For more information refer to <https://support.emc.com/docu55547>. An EMC support account is required. As a result, customers wishing to monitor any VNX array or any CLARiiON CX, CX3, CX4, AX, AX4 series array must use a 7.6.x release of Solutions Enabler.

Configuring Agents to Monitor EMC Storage Arrays (SMI-S)

During this procedure you configure the agent to use SMI-S to collect from the Array Management Host that monitors the arrays. For details, see [Configuring Agents to Monitor Storage Devices](#).

Configuring the SMI-S Provider for EMC CLARiiON or VNX

The SMI-S Provider has a programmatic interface that enables management applications that are integrated with the provider with the ability to discover CLARiiON or VNX storage arrays out of band. This discovery method does not require that a CLARiiON or VNX LUN be visible to the host on which the SMI-S Provider is running—only the IP connection to the storage array is required.

You must provide the following information:

- The IP address of SPA and SPB of the CLARiiON or VNX array to be managed.

- The username and password of the CLARiiON or VNX array that has administrator-level privileges with global scope.

EMC offers the TestSmiProvider tool for adding CLARiiON and VNX arrays to the SMI-S Provider.

- On Windows platforms, the TestSmiProvider.exe resides in c:\program files\emc\ecim\ecom\bin.
- On Linux platforms, TestSmiProvider resides in: /opt/emc/ECIM/ECOM/bin

For more information, see the *SMI-S Provider Release Notes*.

To configure SMI collections for the EMC array:

- 1 Set up the SMI Provider.

The following testsmiprovider program is interactive and provides acceptable defaults. Press return on each line (change the password if needed):

```
C:\Program Files\EMC\ECIM\ECOM\bin>testsmiprovider
Connection Type (ssl,no_ssl,native) [no_ssl]\:
Host [localhost]:
Port [5988]:
Username [admin]:
Password [#1Password]:
Log output to console [y|n (default y)]:
Log output to file [y|n (default y)]:
Logfile path [Testsmiprovider.log]:
(OUTPUT)
Connecting to localhost:5988
Using user account 'admin' with password '#1Password'
#####
## ##
## EMC SMI Provider Tester ##
## This program is intended for use by EMC Support personnel only. ##
## At any time and without warning this program may be revised ##
## without regard to backwards compatibility or be ##
## removed entirely from the kit. ##
#####
slp - slp urls slpv - slp attributes
cn - Connect dc - Disconnect
rc - RepeatCount st - Set timeout value
ns - NameSpace ens - EnumerateNamespaces
ec - EnumerateClasses ecn - EnumerateClassNames
ei - EnumerateInstances ein - EnumerateInstanceNames
a - Associators an - AssociatorNames
r - References rn - ReferenceNames
gi - GetInstance gc - GetClass
lc - Log control dv - Display version info
```

```

ind - Indications menu sl - Start listener
addsys - EMC AddSystem refsys - EMC RefreshSystem
disco - EMC Discover remsys - EMC RemoveSystem
im - InvokeMethod tms - TotalManagedSpace
q - Quit h - Help
#####
Namespace: root/emc
repeat count: 1
(localhost:5988) ?

```

2 Test the provider to be sure it is working.

If you successfully connected to the SMI-S Provider, issue the `dv` command to list basic information about the provider and any attached storage arrays:

```

(localhost:5988) ? dv
++++ Display version information ++++
CIM ObjectManager Name: EMC:10.247.73.48
CIMOM Version: EMC CIM Server Version 2.6.6.1.0.3
SMI-S spec version: 1.4.0
SMI-S Provider version: V4.6.1.0
SMI-S Provider Location: Proxy
SMI-S Provider Server:
Windows_NT l2se0048 6.1.7600 x86_64 (64bit Libraries)
Solutions Enabler version: V7.3-1300 1.0
Retrieve and Display data - 1 Iteration(s) In 0.109006 Seconds

```

a Press the enter key to continue.

i | IMPORTANT: In the above example, the SMI-S Provider is not aware of any attached storage arrays.

3 Add the storage arrays to the provider.

Use the **addsys** command to attach a CLARiiON or VNX array to SMI-S Provider. This command is not for Symmetrix arrays. The following provides an example of attaching an VNX array to the SMI-S Provider:

```

(localhost:5988) ? addsys
Add System {y|n} [n]: y
ArrayType (1=Clar, 2=Symm) [1]:
One or more IP address or Hostname or Array ID
Elements for Addresses
IP address or hostname or array id 0 (blank to quit): 10.247.73.78
IP address or hostname or array id 1 (blank to quit): 10.247.73.79
IP address or hostname or array id 2 (blank to quit):
Address types corresponding to addresses specified above.
(1=URL, 2=IP/Nodename, 3=Array ID)
Address Type (0) [default=2]:
Address Type (1) [default=2]:

```

```

User [null]: clariion
Password [null]: clariion
(OUTPUT)
++++ EMCAddSystem +++++
OUTPUT : 0
Legend:0=Success, 1=Not Supported, 2=Unknown, 3=Timeout, 4=Failed
5=Invalid Parameter, 4096=Job Queued, 4097=Size Not Supported
System :
//10.247.73.48/root/emc:Clar_StorageSystem.CreationClassName="Clar_StorageSystem",Name="CLARiiON+FNM00104500227"

```

In the above example, the first SPA and the SPB of the VNX array is provided. The username/password combination must be of administrator level and global scope.

By issuing the following dv command, you can see the VNX array (which displays as CLARiiON array FNM00104500227) is now present in the provider:

```

(localhost:5988) ? dv
++++ Display version information +++++
CIM ObjectManager Name: EMC:
CIMOM Version: EMC CIM Server Version 2.6.6.1.0.3
SMI-S spec version: 1.4.0
SMI-S Provider version: V4.6.1.0
SMI-S Provider Location: Proxy
SMI-S Provider Server:
Windows_NT l2se0048 6.1.7600 x86_64 (64bit Libraries)
Solutions Enabler version: V7.3-1300 1.0
Firmware version information:
(Remote) CLARiiON Array FNM00104500227 (Rack Mounted VNX7500): 5.31.0.5.006
Retrieve and Display data - 1 Iteration(s) In 0.155009 Seconds

```

a Press the enter key to continue.

- 4 Verify that statistics logging is enabled for your arrays. For more information, see [Verifying Statistics Logging is Enabled on EMC Arrays](#).

- 5 ECOM post-installation tasks

Authentication is required to query the EMC CIM Server. An initial setup is required on the EMC CIM Server to create a CIM user. This can be done using the following procedures:

- a Go to the URL `https://<ipaddress>:5989/ecomconfig`, log in using the username admin and the password #1Password. Or, use the password you created.
- b Click **Add User** and create a user with the role of Administrator. This newly created username can now be used to obtain access to the SMI-S Provider.

Verifying Statistics Logging is Enabled on EMC Arrays

Foglight for Storage Management requires that statistics logging is enabled on an EMC array. Use TestSMIPProvider to verify if statistics logging is enabled for CLARiiON or VNX arrays.

To verify if statistics logging is enabled:

- 1 Log into the server with the SMIs provider installed.
- 2 Run the TestSMIProvider.
- 3 When you reach the point where you can input SMI provider commands, enter:

```
(localhost:5988) ? ei
```

```
Class: cim_statisticsservice
```

- 4 In the output, for the desired array, search for the properties “EnabledState” and “Started”.

If the value for “EnabledState” is “3”, and the value for “Started” is “False”, then statistics logging has not been set for the array, and it will not collect.

The output will display an “instance” for each array, similar to that shown below.

```
Instance 0:
```

```
ObjectPath :
```

```
Clar_BlockStatisticsService.CreationClassName="Clar_BlockStatisticsService",Name="EMCBlockStatisticsService",SystemCreationClassName="Clar_StorageSystem",SystemName="CLARiON+APM001206012345
```

! | **IMPORTANT:** Scroll to the following text.

```
<PROPERTY NAME="EnabledState" CLASSORIGIN="CIM_EnabledLogicalElement" PROPAGATED="true" TYPE="uint16">
```

```
<VALUE>3</VALUE>
```

! | **IMPORTANT:** Scroll to the following text.

```
<PROPERTY NAME="Started" CLASSORIGIN="CIM_Service" PROPAGATED="true" TYPE="boolean">
```

```
<VALUE>FALSE</VALUE>
```

```
</PROPERTY>
```

- 5 If statistics logging is not enabled, see the procedure for the tool you are using:
 - [Enabling Statistics Logging Using Unisphere](#)
 - [Enabling Statistics Logging Using Navisphere](#)

Enabling Statistics Logging Using Unisphere

To enable statistics logging:

- 1 Start Unisphere.
- 2 Select the desired **array**, and select **System**.
- 3 In the System Management tile, click **Properties**.
- 4 On the Storage System Properties dialog box, select the **General** tab.
- 5 Select the **Statistics Logging** check box.
- 6 Click **OK**.

Statistics logging has now been enabled for the array.

- 7 Refresh the SMIS provider using the TestSMIProvider reffsys command.

Enabling Statistics Logging Using Navisphere

To enable statistics logging:

- 1 Start Navisphere.
- 2 Right-click the desired array and click **Properties**.
- 3 On the Storage System Properties dialog box, select the **General tab**.
- 4 Select the **Statistics Logging** check box.
- 5 Click **OK**.
Statistics logging has now been enabled for the array.
- 6 Refresh the SMIS provider using the TestSMIProvider refsys command.

EMC Isilon

Foglight for Storage Management uses the OneFS CLI utility to collect data from all nodes in an EMC Isilon array cluster.

For more information, see the following topics:

- [Requirements for EMC Isilon](#)
- [Configuring Agents to Monitor EMC Isilon Arrays](#)

Requirements for EMC Isilon

- For supported versions EMC Isilon OneFS version, see [Collection Target Support Matrix](#).
- The root account for an Isilon array is required.

Configuring Agents to Monitor EMC Isilon Arrays

Configure an agent for each Isilon array cluster that you want to monitor. For details, see [Configuring Agents to Monitor Storage Devices](#).

EMC VPLEX

Foglight for Storage Management uses the VPLEX Restful APIs to collect data from all nodes in an EMC VPLEX array cluster.

For more information, see the following topics:

- [Requirements for EMC VPLEX](#)
- [Configuring Agents to Monitor EMC VPLEX Arrays](#)

Requirements for EMC VPLEX

- For supported versions EMC VPLEX Local version, see [Collection Target Support Matrix](#).
- The root account for a VPLEX array is required.

Configuring Agents to Monitor EMC VPLEX Arrays

Configure an agent for each VPLEX array cluster that you want to monitor. For details, see [Configuring Agents to Monitor Storage Devices](#).

Hitachi Data Systems AMS, USP, and VSP

Foglight for Storage Management collects information from Hitachi Data Systems Adaptable Modular Storage (AMS), Universal Storage (USP) or Virtual Storage Platform (VSP) using the SMI-S interface of the HiCommand Device Manager component of the Hitachi Command Suite software or the embedded SMI-S provider of VSP arrays.

NOTE: The information in this section applies to all three types of systems: AMS, USP and VSP.

The metrics that can be collected from the standard HiCommand Device Manager are limited. Foglight for Storage Management provides an option to interface with the Hitachi Tuning Manager to collect the following additional metrics.

Table 8. HiCommand Device Manager metrics

Collected Entity	Metric
Disk	Busy (AMS only)
	State (AMS, USP, VSP)
LUN	Bytes Read
	Bytes Written
	Latency
Controller	Busy
Port (Array)	Ops Read
	Ops Write
	Bytes Read
	Bytes Write

For more information, see the following topics:

- [Requirements for Hitachi Data Systems AMS, USP, VSP](#)
- [Configuring Agents to Monitor Hitachi Data Systems AMS](#)

Requirements for Hitachi Data Systems AMS, USP, VSP

Your environment must meet the following requirements:

- The Hitachi HiCommand server is on a different server than Foglight for Storage Management.
- For supported versions of Hitachi Command Suite, see [Collection Target Support Matrix](#).
- **NOTE:** A HiCommand account must explicitly belong to the built-in *Storage Administrator (View Only)* or built-in *ViewGroup* User Group, and must be granted with the VIEW permission.
- The SMI-S component is installed on the Hitachi HiCommand server.
- The SMI-S component is installed on the Hitachi HiCommand server for AMS and USP arrays. For VSP arrays the embedded SMI-S provider must be enabled
- Foglight for Storage Management requires a Command Suite account. By default, all Hitachi Command Suite users are also SMI-S users, so any Command Suite account can be used.
- If you want to collect additional metrics with the Hitachi Tuning Manager:
 - The Hitachi HiCommand server is running on a Windows Server (so that Foglight for Storage Management can collect metrics from the Tuning Manager).
 - The Tuning Manager is enabled on the Hitachi HiCommand server. Tuning Manager is included in Command Suite 7.0 or later, but is licensed separately. For more information, see the *Hitachi Command Suite Installation Guide*.
 - Foglight for Storage Management requires a user account on the Windows Server hosting the Hitachi HiCommand server with the Tuning Manager enabled with the VIEW permission. The account must be configured to run the Tuning Manager.
 - By default CommandSuite (Device Manager) does not automatically refreshes data from Storage Devices that are connected to it. SMI-S is part of the Device Manager, so it does not refresh data as well. In order to make Device Manager refresh data following command below needs to be run on time schedule:

```
HiCommandCLI.bat" http://localhost:2001/service -u system -p manager  
RefreshStorageArrays
```

Configuring Agents to Monitor Hitachi Data Systems AMS

During this procedure, you configure an agent to monitor the server hosting the Hitachi Command Suite. You are prompted to select the arrays to configure. You can also configure the agent to use the Tuning Manager. For details, see [Configuring Agents to Monitor Storage Devices](#).

Configuring Agents to Monitor Hitachi Data Systems USP and VSP Arrays

Monitoring VSP arrays requires a slightly different procedure than monitoring AMS arrays. When monitoring AMS arrays, the SMI-S provider that is part of the Hitachi HiCommand server is used. This is the same server that hosts the Hitachi Tuning Manager. When monitoring USP or VSP arrays however, SMI-S data must be collected from the SMI-S provider embedded in the array itself. The Tuning Manager on the HiCommand server is still used for performance data collection. For details, see [Configuring Agents to Monitor Storage Devices](#).

HP EVA Storage Arrays

Foglight for Storage Management collects information from the HP EVA storage arrays using the SMI-S interface of the SMI-S provider integrated with Command View EVA management software. For procedures describing how to install and configure this component, see the *HP StorageWorks Command View EVA Installation Guide*.

The following versions of HP EVA arrays are supported by Foglight for Storage Management:

3000 Series	5000 Series	8000 Series
4000 Series	6000 Series	8100 Series
4100 Series	6100 Series	8400 Series
4400 Series	6400 Series	

For more information, see the following topics:

- [Requirements for HP EVA Storage Arrays](#)
- [Configuring Agents to Monitor HP EVA Storage Arrays](#)

Requirements for HP EVA Storage Arrays

Your environment must meet the following requirements:

- For supported versions of HP Command View EVA, see [Collection Target Support Matrix](#).
- Foglight for Storage Management is installed on a different server than HP Command View.
- Foglight for Storage Management requires a Command View account. All HP Command View EVA users are also HP SMI-S EVA users, so any Command View account is valid.

Configuring Agents to Monitor HP EVA Storage Arrays

During this procedure, you configure an agent to monitor the server hosting HP EVA Command View. You are prompted to select the arrays to monitor. For details, see [Configuring Agents to Monitor Storage Devices](#).

HP 3PAR Arrays

Foglight for Storage Management collects information from HP 3PAR arrays by communicating with the embedded SMI-S provider integrated into the array's InForm OS.

For more information, see the following topics:

- [Requirements for Dell EqualLogic Arrays](#)
- [Configuring Agents to Monitor Dell EqualLogic Arrays](#)

Requirements for HP 3PAR Arrays

Your environment must meet the following requirements:

- OS version 3.1.2 is required.
- You must enable the SMI-S provider, which is not enabled by default. Use the HP 3PAR CLI.

- Foglight for Storage Management requires an SMI-S account with the Administrator role.

Enabling the SMI-S Provider

To enable the SMI-S provider:

- 1 Log in to the 3PAR CLI using SSH.
- 2 Enter the 3PAR Array IP address.
- 3 Enter the user name configured on the array and the password.
- 4 Enter the command `showcim` to check if the SMI-S provider is already enabled.
- 5 Enter the command `startcim` to enable the SMI-S provider.

For further details, refer to the 3PAR InForm OS Command Line Interface Reference.

Configuring Agents to Monitor HP 3PAR Arrays

During this procedure you create an agent for an HP 3PAR array. The dialog allows you to create multiple agents for other arrays that use the same credentials.

For details, see [Configuring Agents to Monitor Storage Devices](#).

NetApp Filers

Foglight for Storage Management collects storage inventory, data protection, performance, and association information from NetApp filers using the native Data ONTAP API. This requires an integrated account for collecting from NetApp Filers.

- i** **NOTE:** NetApp filers can be configured for both SSLv3 and TLS connections. As a result of recent security changes in Java, the agent will no longer attempt SSLv3 connections when monitoring these systems. If a secure connection is required, TLS must be enabled for the filer. See <https://library.netapp.com/ecmdocs/ECMP1155684/html/GUID-3E07D3F8-6A05-49C0-BF92-9C88BA252E1F.html>

For more information, see the following topics:

- [Requirements for NetApp Filers](#)
- [Configuring Agents to Monitor NetApp Filers](#)

Requirements for NetApp Filers

Your environment must meet the following requirements:

- Foglight for Storage Management requires an account with the appropriate defined role access capabilities to enable DataONTAP® API.
 - For supported versions of DATA ONTAP and Cluster Mode (C-Mode), see [Collection Target Support Matrix](#).
 - For general access, the following permissions are required for the account used for monitoring:
 - login-http-admin - allows connection to the NetApp storage via HTTP.
 - system-api-list - allows querying for the list of available API methods available

- security-api-vfiler - allows the execution of API commands to retrieve vFiler unit information.
- "api-*" - allows the use of NetApp API calls for data collection
- For limited access, different monitoring roles will need to be created depending on the NetApp system to which you are connecting. For information on how to create a read-only user to monitor a storage system in OnCommand System Manager, OnCommand Unified Manager or Performance Advisor, refer to your NetApp documentation. Foglight for Storage Management will never request or require write access to any filer components or services.
- Foglight for Storage Management may execute some or all of the following calls when collecting data. Not all calls are available on all versions of Data ONTAP.

Table 9. List of calls

aggr-get-iter	lun-get-iter	qtree-list
aggr-list-info	lun-get-occupied-size	quota-report
aggr-space-get-iter	lun-get-serial-number	snapshot-delta-info
aggr-status-get-iter	lun-get-space-reservation-info	snapshot-get-reserve
cifs-share-get-iter	lun-list-info	snapshot-list-info
cifs-share-list-iter-end	lun-map-get-iter	snmp-get
cifs-share-list-iter-next	lun-map-list-info	snmp-get-next
cifs-share-list-iter-start	net-interface-get-iter	storage-disk-get-iter
cluster-identity-get	nfs-exportfs-list-rules	system-api-list
disk-list-info	nfs-exportfs-list-rules-2	system-get-info
fcv-adapter-get-iter	perf-object-counter-list-info	system-get-node-info-iter
fcv-adapter-list-info	perf-object-get-instances	system-get-ontapi-version
fcv-interface-get-iter	perf-object-get-instances-iter-end	system-get-version
fcv-node-get-name	perf-object-get-instances-iter-next	vfiler-list-info
fcv-port-name-get-iter	perf-object-get-instances-iter-start	volume-get-iter
igroup-get-iter	perf-object-instance-list-info	volume-get-root-name
iscsi-interface-get-iter	perf-object-instance-list-info-iter	volume-list-info
iscsi-node-get-name	portset-get-iter	volume-options-list-info
iscsi-service-get-iter	portset-list-info	vserver-get-iter

- In **7-Mode**, this command line can be used to create a role with only the limited permissions required for monitoring.

```
useradmin role add vfs_collector -a login-http-admin,api-system-get-version,api-system-get-info,api-system-get-ontapi-version,api-aggr-list-info,api-volume-list-info,api-volume-get-root-name,api-volume-options-list-info,api-qtree-list,api-quota-report,api-disk-list-info,api-cifs-share-list-iter-start,api-cifs-share-list-iter-next,api-cifs-share-list-iter-end,api-nfs-exportfs-list-rules,api-nfs-exportfs-list-rules-2,api-snapshot-delta-info,api-snapshot-get-reserve,api-snapshot-list-info,api-lun-map-list-info,api-lun-list-info,api-lun-get-occupied-size,api-lun-get-space-reservation-info,api-lun-get-serial-number,api-iscsi-node-get-name,api-fcp-node-get-name,api-fcp-adapter-list-info,api-portset-list-info,api-snmp-get,api-snmp-get-next,api-vfiler-list-info,api-perf-object-get-*,api-perf-object-counter-list-info,vfiler-list-info,security-api-vfiler,api-perf-object-instance-list-info,api-system-api-list
```

Once the role is created, it must be associated with a group, and the group associated with a user. The NetApp documentation covers this in more detail:

<https://library.netapp.com/ecmdocs/ECMP1155684/html/GUID-20BAA16F-7411-45F1-84E8-4C6761D9B539.html>

In **cluster mode**, the newer `security login` commands can be used to create a role with the appropriate permissions.

It is possible to create a read-only role and assign it to an account without specifically listing the commands required. This is done by first creating the role with the correct access permissions, and then creating a new user account associated with that role.

To create the rule, the following command is used:

```
security login role create -role vfs_collector -cmddirname DEFAULT -
access readonly
```

This role will have read-only access to the default set of NetApp commands. Then a user can be created and associated with this role:

```
security login create -username vtest -application ontapi -authmethod
password -role vfs_collector
```

If more fine-grained control over the permissions assigned is required, then the complete list of commands required will need to be granted individually. This is done by allowing read-only access to the command associated with each API call that the Foglight for Storage Management agent is required to make. The NetApp documentation should be consulted for more details.

The mapping of API permissions to NetApp commands is:

Table 10. Mapping of API permissions to NetApp commands

API Name	Command Line Permission
api-aggr-get-iter, api-aggr-status-get-iter	storage aggregate show
api-aggr-space-get-iter	storage aggregate show-space
api-cifs-share-get-iter	vserver cifs share show
api-cluster-identity-get	cluster show
api-disk-list-info	storage disk show
api-fcp-adapter-get-iter	network fcp adapter show
api-fcp-interface-get-iter	vserver fcp interface show
api-fcp-port-name-get-iter	vserver fcp wwpn-alias show
api-iscsi-service-get-iter	vserver iscsi show
api-lun-get-iter	lun show
api-lun-map-get-iter	lun mapped show
api-net-interface-get-iter	network interface show
api-nfs-service-get-iter	vserver nfs show, vserver nfs status
api-perf-object-counter-list-info	statistics catalog counter show
api-perf-object-get*	statistics show
api-perf-object-instance-list-info-iter	statistics catalog instance show
api-portset-get-iter	lun portset show
api-qtree-list-iter	volume qtree show
api-quota-report-iter	volume quota report
api-snapshot-*	volume snapshot show, volume snapshot policy show
api-storage-disk-get-iter	storage disk show
api-system-get-node-info-iter	system node image show
api-system-get-version	version
api-volume-get-iter	volume show

Table 10. Mapping of API permissions to NetApp commands

API Name	Command Line Permission
api-vserver-get-iter	vserver show
igroup-get-iter	lun igroup show

A new role should be created:

```
security login role create -role vfs_collector -cmddirname "security
login role show-ontapi" -access readonly
```

Each of the command line permissions will need to be assigned to the selected role in the following manner:

```
security login role create -role vfs_collector -cmddirname "storage
aggregate show" -access readonly
```

Then a user created and associated with that role:

```
security login create -role vfs_collector -username vtest -application
ontapi -authmethod password
```

Configuring Agents to Monitor NetApp Filers

Configure an agent for each NetApp filer you want to monitor. For details, see [Configuring Agents to Monitor Storage Devices](#).

Collection Target Support Matrix

The following configurations of FC Switches, Filers, and Storage Arrays are supported on the Foglight for Storage Management:

Table 11. Support matrix

		Supported platforms	Supported latest GA
FC Switches	Brocade	Brocade Network Advisor (BNA)	BNA 14.0.1
	Cisco	MDS 9000 up to MDS 9700 Series	N/A
		Nexus 5000 Series	N/A
Filers	NetApp	NetApp Filer 7-Mode	DATA ONTAP 7.X up to 8.1.1
		NetApp Filer Cluster Mode (C-Mode)	DATA ONTAP 8.X up to 9.2
		NOTE: Metro Cluster is not supported.	

Table 11. Support matrix

		Supported platforms	Supported latest GA
Storage Arrays	Dell Compellent	Dell Enterprise Manager (EM)	EM 2015 R3 (Build 15.3.1.300)
		Dell Storage Manager (DSM)	DSM 2016 R2
	Dell EqualLogic	PS Series group NOTE: FS7600 series NAS appliance is not supported.	Firmware 6.0
	EMC CLARiiON/VNX CLI	EMC NaviSphere Command Line Interface (CLI)	NaviSphere CLI 7.33.9.1
	EMC CLARiiON/VNX/VMAX SMIS	EMC SMI-S Provider NOTE: VNXe series is not supported.	
		CLARiiON CX4 CLARiiON AX4 CLARiiON AX150 VNX ALL	<ul style="list-style-type: none"> Supported latest solutions Enabler GA: 7.6.2 Supported latest SMI-S GA: 4.6.2
		Symmetrix VMAX 10K Symmetrix VMAX 20K Symmetrix VMAX 40K	<ul style="list-style-type: none"> Supported latest solutions Enabler GA: 8.3.0 Supported latest SMI-S GA: 8.3
	EMC Isilon	EMC Isilon OneFS	Isilon OneFS version 7.2.1 Isilon OneFS version 8.0
	EMC VPLEX	EMC VPLEX Local	GeoSynchrony 5.5 and higher
	HDS AMS/USP/VSP	Hitachi Command Suite NOTE: HUS array is not supported.	HCS V8.5.1
HP EVA	HP StorageWorks Command View	HP StorageWorks Command View EVA v9.04	
HP 3PAR	HP 3PAR InServ F400	N/A	
Generic SMI-S Array	Dot Hill	Dothill Assured SAN 5720 (Seagate)	N/A
	EMC Unity	Unity 300	4.1.2.9257522
		Unity 400F	4.1.2
	Fujitsu	Fujitsu ETERNUS DX200S3 and DX80S2	N/A
	HP	HP P2000 MSA and P2040 MSA	N/A
	Huawei	OceanStor V3 Series	V3R6 and later
OceanStor Dorado		V3 Series V3R1 and later	
OceanStor V5 Series		V5R7 and later	

Configuration Procedures

The preceding sections link to the following configuration procedures:

- [Configuring Agents to Monitor Storage Devices](#)
- [Assigning Credentials](#)
- [Resolving Connection Attempt Errors](#)
- [Configuring the Hitachi Tuning Manager](#)
- [Configuring Generic SMI-S Array Agent to Monitor Storage Devices](#)

Configuring Agents to Monitor Storage Devices

To configure an agent to monitor the storage device:

- 1 On the navigation panel, under **Homes**, click **Storage Environment**.
- 2 Click the **Administration** tab.
- 3 Click **Configure Agent for Storage Device Monitoring**.
The Storage Device Setup dialog opens.
- 4 In the **Add/Edit Agent** section, select an agent manager host from the *Agent Manager* drop-down list.
- 5 In the **Add/Edit Agent** section, configure the agent settings:
 - a Select the type of storage device from the *Resource Type* and *Model* drop-down lists, as indicated in [Table 12](#).
 - b In the *IP Address* field, type the IP address of the server hosting the agent manager.
 - c If the Agent uses a non-default port, type the port number in the *Port* field. Ensure that this port is open and that traffic is permitted between the device and the Agent Manager host.
 - d Specify a name for the agent in the *Name* field (optional).
 - e Click **Add**.

The system checks the IP address. If the validation fails, check the IP address and ensure the device at the IP address is functioning.

The Credential Assignment Wizard opens.

- 6 Create or select a credential that contains the account information needed to access the storage device. For detailed information, see [Assigning Credentials](#).
- 7 For Hitachi Data Systems AMS, USP, and VSP devices only: If you want to use the Hitachi Tuning Manager for collecting additional metrics, follow the instructions in [Configuring the Hitachi Tuning Manager](#).
The new StorageAgentMaster Monitor Agent is added to the table at the bottom of the dialog.
- 8 If the agent is correctly configured, continue with [Step 9](#).
If the agent is incorrectly configured, the *Validated* column provides details to help you troubleshoot the issue. For additional information, see [Resolving Connection Attempt Errors](#).
- 9 Click **OK** to exist the Storage Device Setup dialog.

Table 12. Storage Device requirements

Type of Storage Device	Vendor	Resource Type field	Model field
FC Switches	Brocade SAN Switches	FC Switch	Brocade
	Cisco SAN Switches	FC Switch	Cisco
Storage Arrays	Dell Compellent Arrays	Storage Array	Dell Compellent
	Dell EqualLogic PS Series Array Groups	Storage Array	Dell EqualLogic
	EMC CLARiiON CX Series Arrays (CLI)	Storage Array	EMC CLARiiON using CLI
	EMC CLARiiON, VNX, or VMAX Storage Arrays (SMI-S)	Storage Array	EMC VNX/CLARiiON/VMAX - SMIS
	EMC Isilon	Storage Array	EMC Isilon
	Hitachi Data Systems AMS, USP, and VSP	Storage Array	HDS AMS/UPS/VSP
	HP EVA Storage Arrays	Storage Array	HP EVA
	HP 3PAR Arrays	Storage Array	HP 3PAR
Filers	NetApp Filers	Filer	NetApp

Assigning Credentials

When configuring an agent to monitor a storage device, you need to assign a credential. Here are some typical scenarios:


- A storage device has a unique account and password. Create a credential to contain the account and password and assign it to this device only.
- Multiple storage devices of the same type are configured to use the same account and password. The first time you configure a Storage Collector Agent to monitor one of these devices, create and assign a credential that contains the account and password. When configuring additional agents to monitor the rest of the devices, select and assign this existing credential to the devices.
- A single storage device has multiple accounts that can be used to access it. When you configure a Storage Collector Agent to monitor this device, create and assign a credential for each account. When the Storage Collector Agent attempts to authenticate itself with the device, it tries the credentials one at a time until it connects successfully. Any remaining credentials are not tried.

This section contains procedures that describe how to create or select a credential. It also contains information about releasing Agent Manager lockboxes.

- [Creating and assigning new credentials](#)
- [Selecting and assigning an existing credential](#)
- [About releasing the Agent Manager lockbox](#)

Creating and assigning new credentials

To create a new credential:

- 1 In the Credential Assignment Wizard, click **New Credential - Create and Assign**.
The available options differ slightly depending on the storage device.
- 2 In the Unique Name field, type a name that is unique to this credential.
- 3 If the Domain box is displayed, type the domain.
 **IMPORTANT:** If the Domain box is not displayed, and you need to specify the domain, include the domain as part of the account name.
- 4 Do one of the following:
 - If the **Account Name and Password** boxes are displayed, provide user credentials for the target application and/or the target server hosting the management application.
 - If the **SNMP Community String** box is displayed, type the SNMP community name assigned to the storage array group that you want to access.
- 5 In the Select the lockbox to contain this credential table, select a Foglight lockbox to contain this credential. For more information, see [Creating a Lockbox for Foglight for Storage Management Credentials](#).
- 6 Click **Submit**.
The Credential Assignment Wizard page is updated to display the new credential.
- 7 For Hitachi Data Systems AMS, USP, and VSP devices, click Next to continue with [Configuring the Hitachi Tuning Manager](#). For all other device types, click **Finish** to return to the Storage Device Setup dialog.

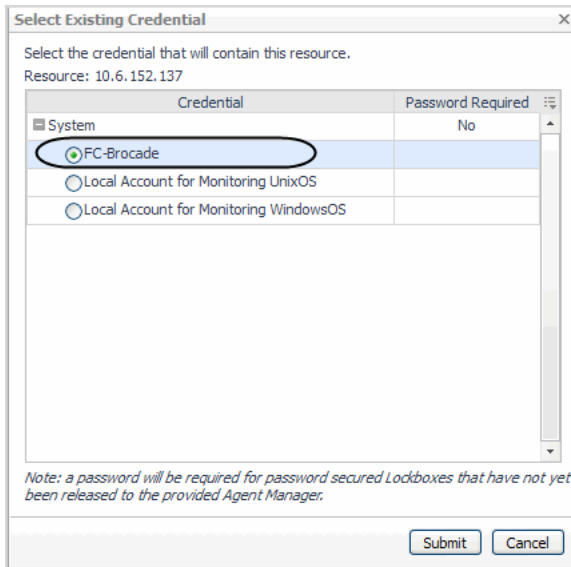
Selecting and assigning an existing credential

To select and assign existing credentials:

- 1 In the Credential Assignment Wizard, click **Existing Credential - Select and Assign**.


The Select Existing Credential dialog box opens.

- 2 Select the credential to use with the target storage device.



- 3 Click **Submit**.

The Credential Assignment Wizard page is updated to display the assigned credential.

- 4 If this is the first agent to use a credential in the lockbox, in the row containing the lockbox, click  **Release Lockbox**. If prompted, enter the lockbox password.
- 5 For Hitachi Data Systems AMS, USP, and VSP devices, click **Next** to continue with [Configuring the Hitachi Tuning Manager](#). For all other device types, click **Finish** to return to the Storage Device Setup dialog.

About releasing the Agent Manager lockbox

An Agent Manager lockbox needs to be released the first time an agent is deployed to the Agent Manager host. This releases the lockbox to the client Agent Manager Host, making all the credentials in the lockbox available to the agents on that host. You can release the lockbox from the Storage Device Setup wizard, the Edit Agent Properties dialog box, or from the Credentials dashboard.

Resolving Connection Attempt Errors

If the agent's attempt to connect and validate fails, the error message usually contains a suggested resolution. For example, you may need to fix credentials or release the lockbox.

If the connection is refused because the entered IP address is incorrect, you need to cancel the wizard, delete the agent, and restart the wizard using the correct IP address. If the port is wrong, you can click the value beside the Port field to correct the value.

If the problem cannot be resolved at this time, close the Storage Device Setup dialog. The configuration that has been done up to the point where the error occurred is saved. After resolving the problem, edit the agent configuration and validate the settings. For more information, see [Editing Configured Agents](#).

Configuring the Hitachi Tuning Manager

To configure the Hitachi Tuning Manager:

- 1 On the second page of the Credential Assignment Wizard (available only for Hitachi Data Systems AMS, USP, and VSP devices), read the information provided.
- 2 If you want to use the Hitachi Tuning Manager for collecting additional metrics, check the **Use HDS Tuning Manager** checkbox.
- 3 If the Tuning Manager is not installed in the default path, type the installation *Path*.
- 4 Type the *IP Address* of the system on which HDS Tuning is installed. If left blank, then the IP address of the array or array manager is assumed.
- 5 Click **Finish** to complete the operation and return to the Storage Device Setup dialog.

Configuring Generic SMI-S Array Agent to Monitor Storage Devices

During this procedure, you configure the agent to use SMI-S to collect from the Array Management Host that monitors the arrays.

To configure an agent to monitor the storage device:

- 1 On the navigation panel, under **Dashboards**, click the **Administration > Agents > Agent Status** tab.
- 2 Click **Deploy Agent Package**.

The **Storage Device Setup Wizard** opens. Each of the following steps corresponds to one page in the wizard. Use the **Next** and **Back** buttons to navigate between pages.

- a On the *Select Host Selector* page, select the Host to host this agent.
- b On the *Select Agent Packages* page, select **SMISStorageAgent**.
- c On the *Agent Configuration Summary* page, review the agent configuration. You can go back and make corrections, if necessary.
- d Click **Finish**.

- 3 Click **Create Agent**.

The **Storage Device Setup Wizard** opens. Each of the following steps corresponds to one page in the wizard. Use the **Next** and **Back** buttons to navigate between pages.

- a On the *Select Host Selector* page, select the Host to host this agent.
- b On the *Select Agent Type and Instance* page, select **SMISStorageAgent**.
- c On the *Agent Configuration Summary* page, review the agent configuration. You can go back and make corrections, if necessary.
- d Click **Finish**.

- 4 Select the Agent to configure, click **Edit Properties**.
- 5 Modify the private properties for this agent.
- 6 Edit the following user-defined Properties, as needed:
 - Host: ip of the SMI-S, default 127.0.0.1
 - Port: port of the SMI-S, default 5989
 - Username: the user of the SMI-S
 - Password: the password of the SMI-S

- 7 Click **Save**.
- 8 Select the Agent that you want to activate, and then click **Activate**.

Managing Agents

After you create agents, you can check their status and alarms. Over time, you may need to edit configured agents. You complete these tasks on the Storage Environment dashboard under the Administration tab.

This section covers the following tasks:

- [Reviewing the Status of Configured Storage Collector Agents](#)
- [Reviewing Agent Alarms](#)
- [Editing Configured Agents](#)
- [Deploying Storage Agents after an Upgrade](#)

Reviewing the Status of Configured Storage Collector Agents

The Storage Collector Agents view displays all Storage Collector agents, their status, and current alarms on that agent.

If the **Configured** box is not checked, some aspect of the configuration is incorrect. The agent has not validated successfully and is unable to collect data. To correct the configuration, see [Editing Configured Agents](#).

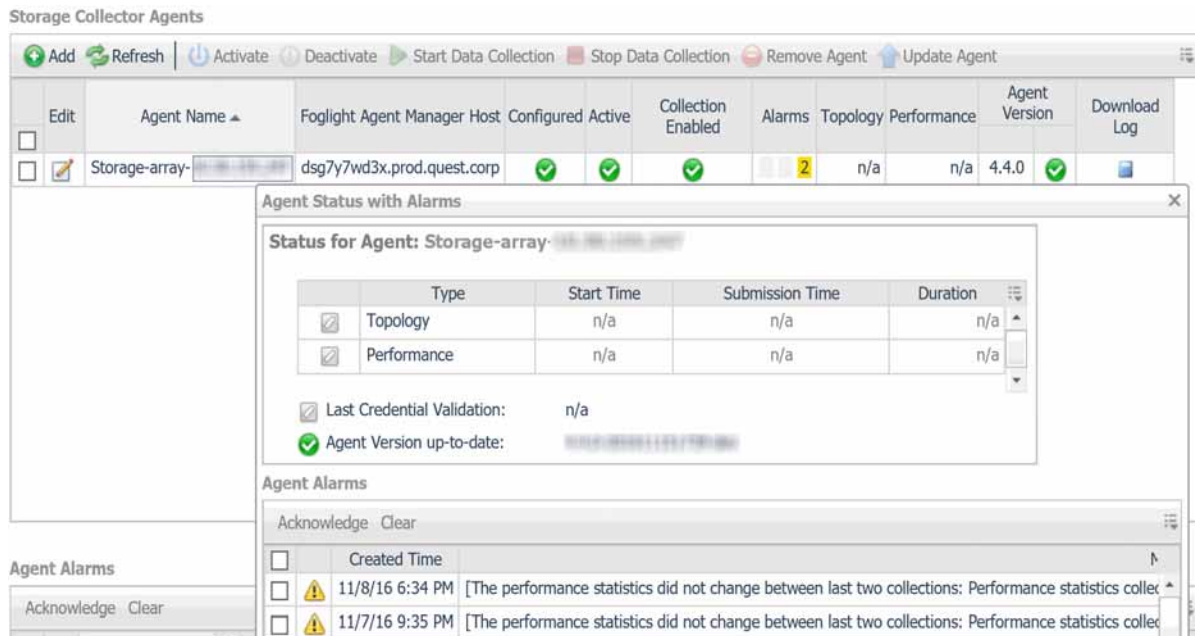
Figure 2. Storage Collector Agents view

Edit	Agent Name	Foglight Agent Manager Host	Configured	Active	Collection Enabled	Alarms	Topology	Performance	Agent Version	Download Log
	Brocade	delta-fms-vm.vf.fstc.us.qfif	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		4/10/17 7:49 PM	4/10/17 8:33 PM	4.6.5	
	Compellent	delta-fms-vm.vf.fstc.us.qfif	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		4/10/17 7:48 PM	4/10/17 8:33 PM	4.6.5	
	EMC-CLI	delta-fms-vm.vf.fstc.us.qfif	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		4/10/17 7:49 PM	4/10/17 8:33 PM	4.6.5	
	Equallogic	delta-fms-vm.vf.fstc.us.qfif	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		4/10/17 7:48 PM	4/10/17 8:33 PM	4.6.5	
	HP-EVA	delta-fms-vm.vf.fstc.us.qfif	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		4/10/17 7:48 PM	4/10/17 8:33 PM	4.6.5	
	mds9148-1	delta-fms-vm.vf.fstc.us.qfif	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		4/10/17 7:48 PM	4/10/17 8:33 PM	4.6.5	
	mds9148-2	delta-fms-vm.vf.fstc.us.qfif	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		4/10/17 7:49 PM	4/10/17 8:33 PM	4.6.5	
	USP-41	delta-fms-vm.vf.fstc.us.qfif	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		4/10/17 7:49 PM	4/10/17 8:03 PM	4.6.5	

Reviewing Agent Alarms

The Agent Alarms view shows the alarms that have been triggered, but not cleared for the Storage Collector agents. Failure to fix a chronic problem may cause the agent to stop collecting data. Note the following:

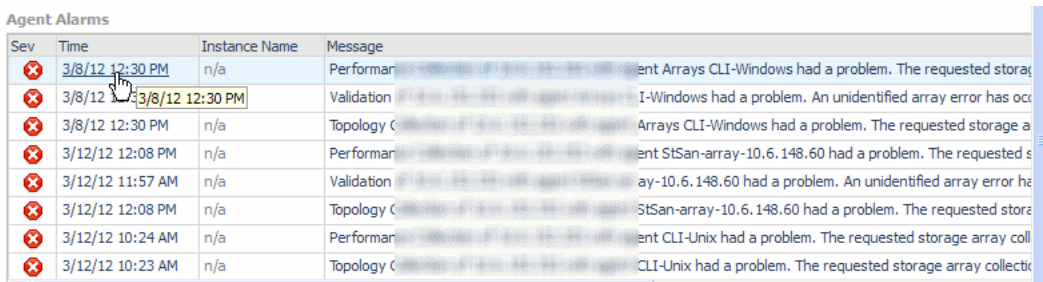
- A Storage Collector agent alarm typically indicates a collection failure, and provides the reason for the failure.
- A typical failure cause is that a password has been changed for a storage device, but the password in the associated credential has not been changed, leading to an authentication failure.
- If you frequently get an alarm indicating a collection has timed-out, consider changing the agent schedule to collect less frequently. The Status panel on the Edit Agent Properties dialog box displays the duration of the last collection.



From this table you can select an alarm to view the alarm details.

To view alarm details or administer alarms:

- 1 Click on the required alarm.



The alarm message box opens.

- 2 After performing the required task, click **Cancel**.

The alarm message box closes.

Editing Configured Agents

The Edit Agent Properties dialog box provides the following functions for all configured agents:

- View collection times and status.

- Assign/Edit credentials.
- Validate device connectivity.

The following functions are provided if relevant for a specific device type:

- Edit port or path properties.
- View the target devices being collected via a management host.
- Enable/disable the collection of specific arrays via a management host.
- Hitachi—enable/disable the use of the Tuning Manager.
- CLARiiON using CLI—discover arrays in new domains.
- Discover new arrays/switches in the environment using the Validate Connectivity function.

To edit Foglight for Storage Management Agent properties:

- Click the **Edit** icon to the left of the Agent Name to open the Edit Agent Properties view.

The Agent Properties Editor page opens.

From the Edit Properties dialog box, you can perform the following tasks:

- [Reviewing Agent Status and Validating Connectivity](#)
- [Managing Credentials](#)
- [Managing Discovered Switches and Arrays](#)
- [Managing CLARiiON Domains and Arrays](#)
- [Managing the Hitachi Tuning Manager](#)

Reviewing Agent Status and Validating Connectivity

The Status tab displays the agent status and the properties status of the selected device.

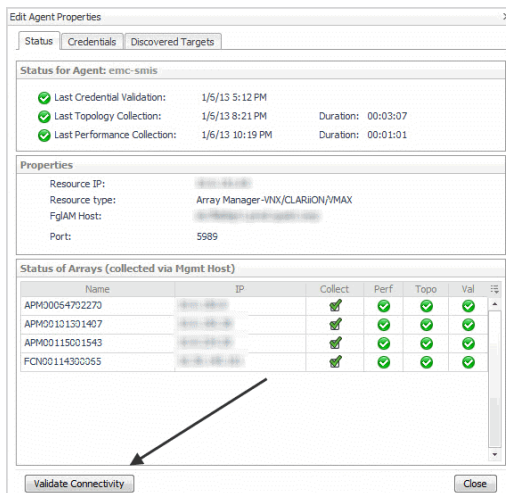
Validating Connectivity

Use the **Validate Connectivity** button to verify that the agent can still connect to the device with changed properties.

Use the Validate Connectivity button to discover new devices managed by existing management hosts. The agent configured to collect from a management host will discover new managed devices, and add them to the discovered targets for collection.

The Validate Connectivity button is visible at the bottom of the dialog box.

Figure 3. Edit Agent Properties



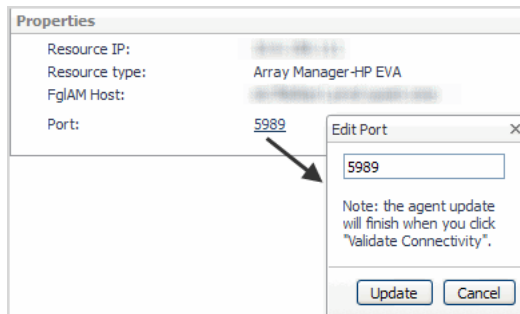
Properties Panel

The Properties view varies based upon the agent type.

Port Property

Agents that allowed port configuration in the wizard display the port.

Figure 4. Port Property



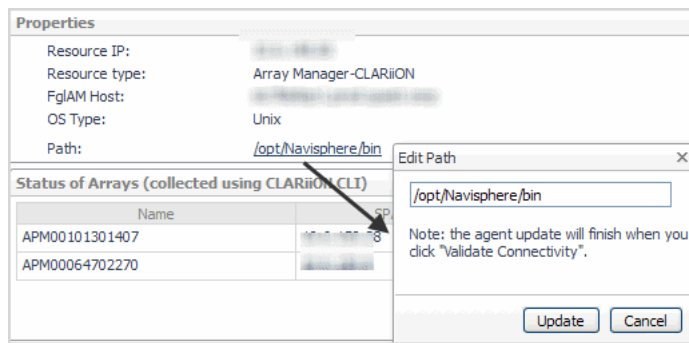
To change the port:

- 1 Click the port number to open the Edit Port dialog box.
- 2 Enter the new port value, or clear the field to reset it to the default.
- 3 Click **Update**.
- 4 Click **Validate Connectivity** before you close the Edit Agent Properties dialog box.

Path Property

CLARiiON monitoring using CLI displays a path property.

Figure 5. Path Property



To change the path:

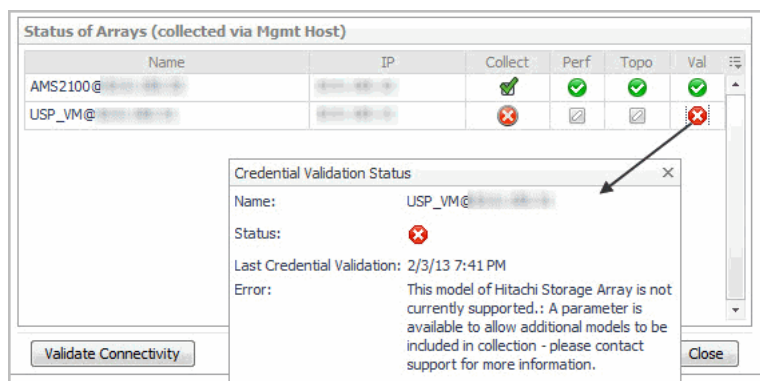
- 1 Click on the path to open Edit Path dialog box.
- 2 Enter the new path value, or clear the field to reset it to the default.
- 3 Click **Update**.
- 4 Click **Validate Connectivity before you close** the Edit Agent Properties dialog box.

Status of Arrays

This view displays as part of the Status tab only when collecting arrays. The upper **Status for Agent** panel displays the success/failure in connecting to the array management host.

Each row in this panel displays whether the array is configured for collection, and the status of the last collection attempt to that array. Clicking on the status icon displays the popup that provides error information, if the status was not successful.

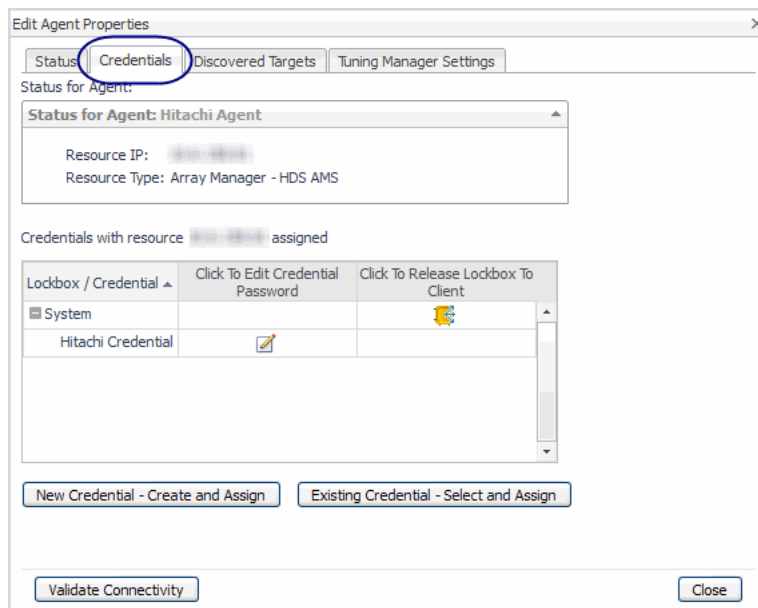
Figure 6. Credential Validation Status



Managing Credentials

This tab displays the credentials for the selected agent.

Figure 7. Managing Credentials



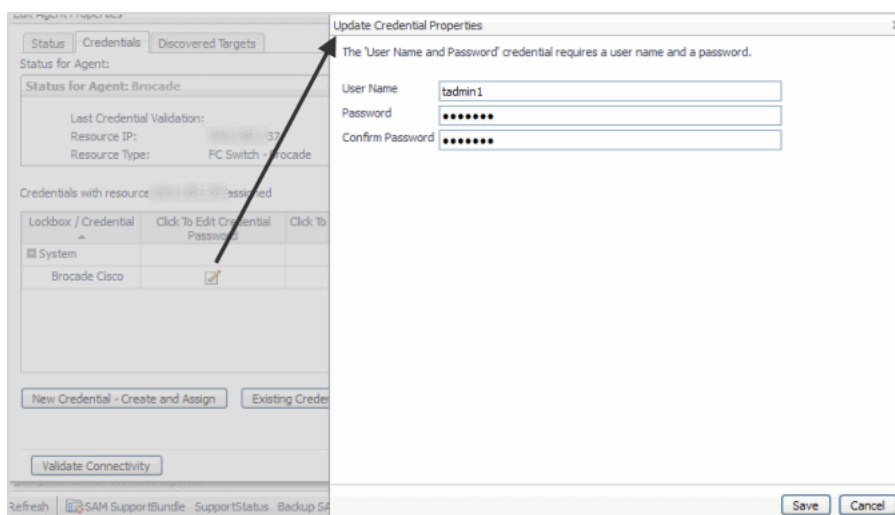
From this tab you can create or select credentials. For procedures, see [Assigning Credentials](#). You can also edit the password for a credential.

To delete an obsolete credential, remove obsolete mappings, or to manage lockboxes, use the Credentials dashboard. To access this dashboard, on the navigation panel, under Dashboards, click **Administration > Credentials**. For help with the dashboard, see the online help.

Editing existing credentials

To edit the password:

- 1 In the row contain the target credential, click the **Edit** icon.



- 2 Modify the credentials as required.
- 3 Click Save.
- 4 From the Credentials tab, click **Validate Connectivity** to ensure that the storage device can be accessed with the changed credentials.

If the test is unsuccessful, an error is reported.

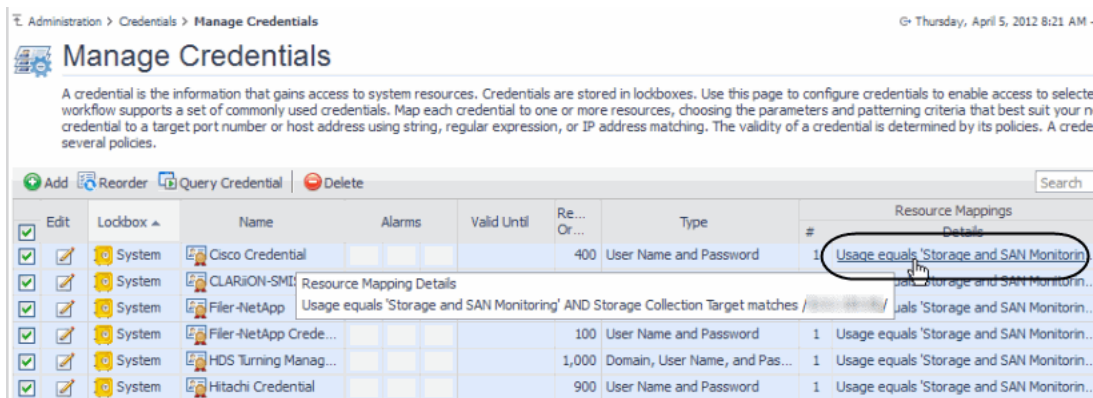
For more information, click the word Error. The Errors Were Found window opens with a description of the errors.

Removing a resource mapping from the Credentials dashboard

When a credential is used for multiple storage devices, you can remove storage devices from the credential when it is no longer valid.

To remove a resource mapping credential:

- 1 On the navigation panel, under Dashboards, click **Administration > Credentials**.
The Credentials view displays.
- 2 Click **Manage Credentials**.
- 3 In the Resource Mappings column, click the storage device you want to remove.



The Update Resource Mapping of Credential page opens.

- 4 Click the **Remove** icon for the required resource.
- 5 When prompted for confirmation, click **Confirm**. The mapping credential is deleted.
- 6 Click **Save**.

The credential is removed from the Manage Credentials view.

Managing Discovered Switches and Arrays

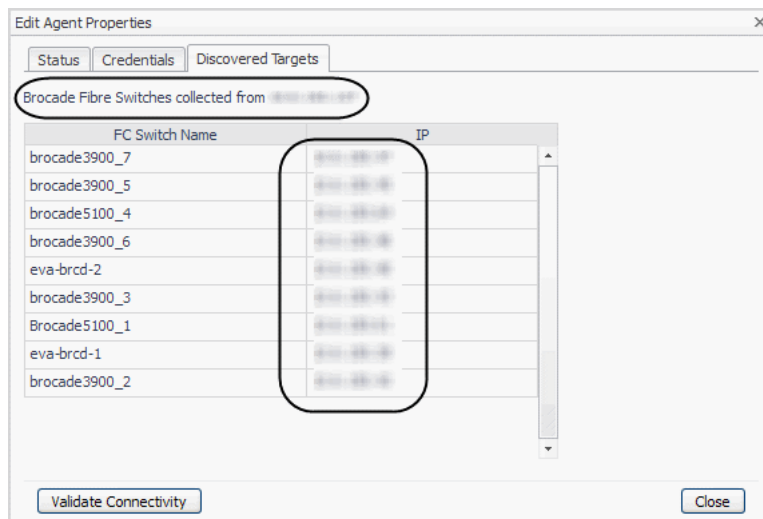
The Discovered Targets tab shows the storage devices that are collected through a management resource. The following tabs are provided:

- [Brocade Discovered Targets Tab](#).
- [Arrays Discovered Targets Tab](#).

Brocade Discovered Targets Tab

For Brocade switches, this view displays all FC switch names and IP addresses that are being monitored by this agent through the management host.

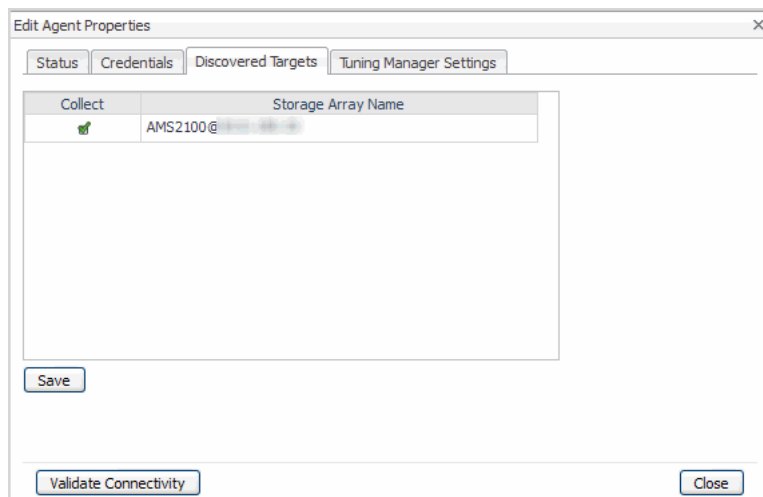
Figure 8. Discovered Targets tab



Arrays Discovered Targets Tab

From this page, you can change which arrays should or should not be collected through the management host.

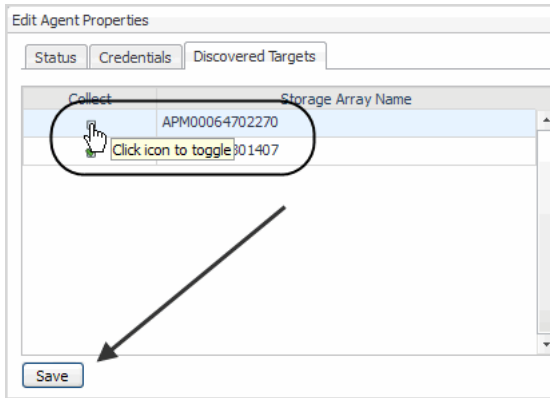
Figure 9. Arrays Discovered Targets tab



The following procedures allow you to disable/enable arrays from being monitored.

Disable/Enable Array Targets

- 1 Click the storage array name so the corresponding icon is checked or cleared, and click **Save**.



The Saving message box displays error messages.

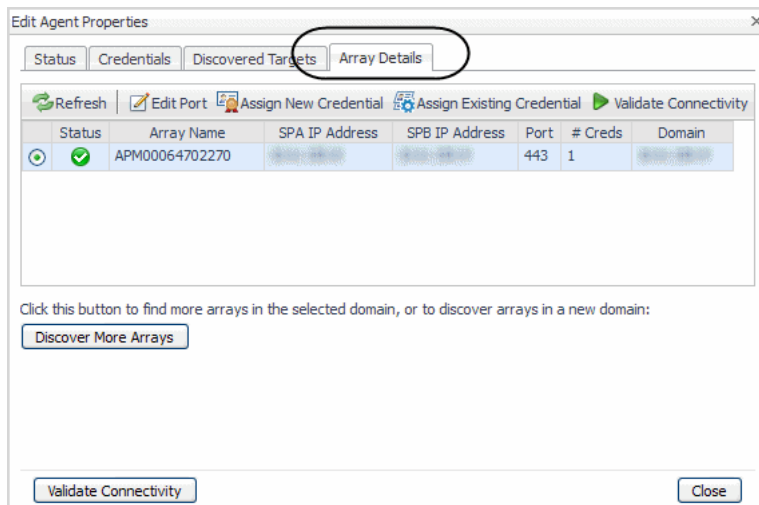
- 2 Click **OK**.

The properties are saved.

Managing CLARiON Domains and Arrays

The Array Details tab allows you to discover arrays in additional domains, and rediscover new arrays added to existing domains. For more information, see [EMC CLARiON CX Series Arrays \(CLI\)](#).

Figure 10. Array Details



Managing the Hitachi Tuning Manager

The HDS Tuning Manager Settings tab allows you to enable or disable collection from the Hitachi Tuning Manager (on Windows). For information about Hitachi Tuning Manager requirements and metrics, see [Hitachi Data Systems AMS, USP, and VSP](#).

Figure 11. HDS Tuning Manager Settings



From this tab you can edit settings for the HDS Tuning Manager.

To enable the Tuning Manager:

- 1 Click **Edit Settings for HDS Tuning Manager**.
The Edit Tuning Manager Settings dialog box opens.
- 2 Select the **Use HDS Tuning Manager** check box. Provide a path if the HDS Tuning Manager is not installed at the default location. (This example shows a non-default path).



- 3 Create a new credential or assign an existing credential to access the Tuning Manager. For help on this task, see [Assigning Credentials](#).
- 4 Click **Save**.
The Updating and Validating Connectivity message box opens.
- 5 If the validation completes with no errors, click **OK**, then click **Cancel** to exit this dialog box.
If the validation encounters an error, click the **Error** label to display the error. Fix the problem, then click **Save** to try and validate again.

To disable the Tuning Manager:

- 1 Click **Edit Settings for HDS Tuning Manager**.
The Edit HDS Tuning Manager Settings dialog box opens.

- 2 Clear the **Use HDS Tuning Manager** check box.
- 3 Click **Save**.
- 4 In the Updating and Validating Connectivity message box, click **OK**.
- 5 Click **Cancel** to exit this dialog box.

Deploying Storage Agents after an Upgrade

After the StorageCollector cartridge is updated, (using the Installed Cartridge dashboard), it needs to be deployed to the Agent Manager(s) that have agents of this type. Deployment should be done from the Storage Environment Administration dashboard.

Using the Update Agent function on the Storage Environment Administration tab will ensure that updates to the StorageCollector agent remain in synch with updates to the embedded database.

After the upgrade completes successfully, the Storage Collector Agents view may show that the agents are not active. This is a temporary state, while the agents are being upgraded with the new code.

The screenshot shows the 'Storage Environment Administration' dashboard. At the top, there are tabs for Monitoring, FAQs, Reports, Storage Capacity, Administration, and Getting Started. Below the tabs is a 'Tasks' section with a list of tasks: Configure Agent for Storage Device Monitoring, Change Alarm Sensitivity, Configure Storage Administrator Email Addresses, Enable Physical Host to Storage Dependency Processing, Update Disk Models, Review Instances and Alarms, and Configure Duplicate Alarms. Below the tasks is a 'Storage Collector Agents' section with a table of agents. The table has columns for Edit, Agent Name, Foglight Agent Manager Host, Configured, Active, Collection Enabled, Alarms, and Topology. The table contains two rows: AMS-USP and Brocade, both with 'Configured' and 'Collection Enabled' status as 'Yes' and 'Active' status as 'No'.

Edit	Agent Name	Foglight Agent Manager Host	Configured	Active	Collection Enabled	Alarms	Topology
<input type="checkbox"/>	AMS-USP	delta-fms-vm4.vfs.stc.us.qsft	Yes	No	Yes	n/a	
<input type="checkbox"/>	Brocade	delta-fms-vm4.vfs.stc.us.qsft	Yes	No	Yes	n/a	11/9/16 3:55 f

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit <https://www.quest.com/company/contact-us.aspx> or call +1-949-754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.