Quest™

Foglight® for Storage Management 6.0.0
User and Reference Guide

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.**

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

Contents

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 configure Foglight for Storage Management.

This workflow has the following steps:

1 Introducing Foglight for Storage Management

2 Navigating Foglight for Storage Management

3 Introducing the Storage Monitoring Architecture

4 Sizing Your Monitored Environment

5 Ensuring System Requirements are Met

6 Configuring Agent Managers for Storage Collection

7 Supporting an Environment with Separate Fabrics that have Duplicated WWNs

8 Configuring Storage Collector Agents

9 Configuring VMware Performance Agents

10 Configuring Hyper-V Agents

11 Assigning Foglight for Storage Management Roles

Introducing Foglight for Storage Management

Virtual infrastructures add layers of abstraction that obscure the relationship between physical storage and virtual machines. Foglight for Storage Management supports VMWare and Hyper-V virtual environments. It helps you look beyond logical datastores and volumes to see how physical storage components (switches, logical unit numbers (LUNs), arrays, and filers) are impacting virtual machines (VMs).

The key concepts for Foglight for Storage Management are "relationship" and "context." Rather than simply viewing repeated performance metrics, Foglight for Storage Management incorporates the data into an end-to-end view of your virtual storage infrastructure, showing the relationship of the storage and storage area network (SAN) performance to VM performance. You can also investigate performance events in the proper context, viewing the status of the entire topology at the time the performance issues occurred.

Performance Monitoring

Monitoring the performance of your storage infrastructure is critical to maximizing VM performance. Foglight for Storage Management allows you to track:

• Insufficient bandwidth and throughput of SAN switch ports, filers, and storage arrays.

• Over (or under) utilized datastores CSVs, and logical disks.

- I/O bottlenecks for NASVolumes and LUNs, along with the pool providing the physical disk storage for the LUNs and NASVolumes.

Figure 1. Performance Monitoring
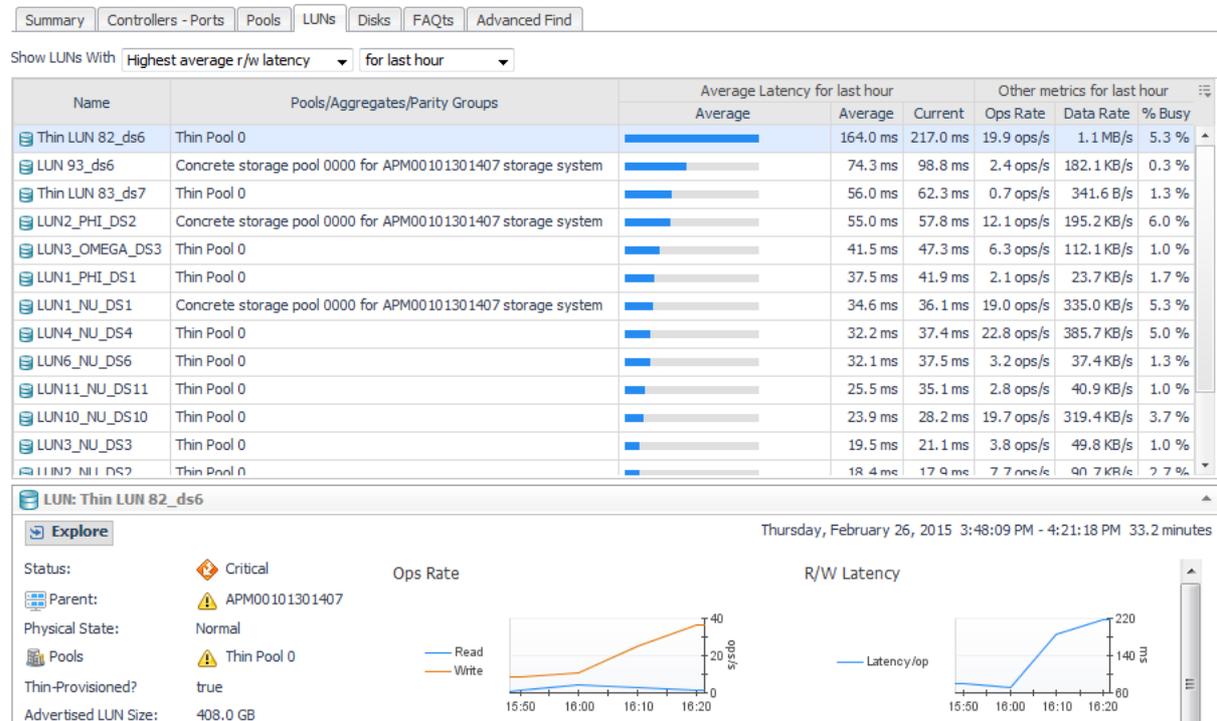
Foglight for Storage Management captures performance metrics from components of your storage infrastructure (SAN switches, LUNs, storage arrays, and filers), evaluates the data based on preconfigured performance and event rules, then presents this data via a detailed graphical interface. With architectural diagrams, graphs, alerts, and drill-down screens, Foglight for Storage Management helps you quickly identify problems in the virtual environment or the physical storage. For more information, see Summary and Resource Information for each Collected Target:.

Capacity Monitoring

Foglight for Storage Management aids the process of identifying and resolving storage capacity issues. The Foglight for Storage Management virtualization cartridges alert you to datastores and logical volumes in danger of running out of storage. The storage component shows you how the physical storage supporting your virtual infrastructure is configured. The detailed graphical interface of Foglight for Storage Management lets you see storage capacity allocations for arrays and filers, and receive alerts when free disk capacity and free pool capacity fall below thresholds. For more information, see Monitoring Storage Arrays, Monitoring Filers, and Monitoring Storage Capacity.

Figure 2. Capacity Monitoring
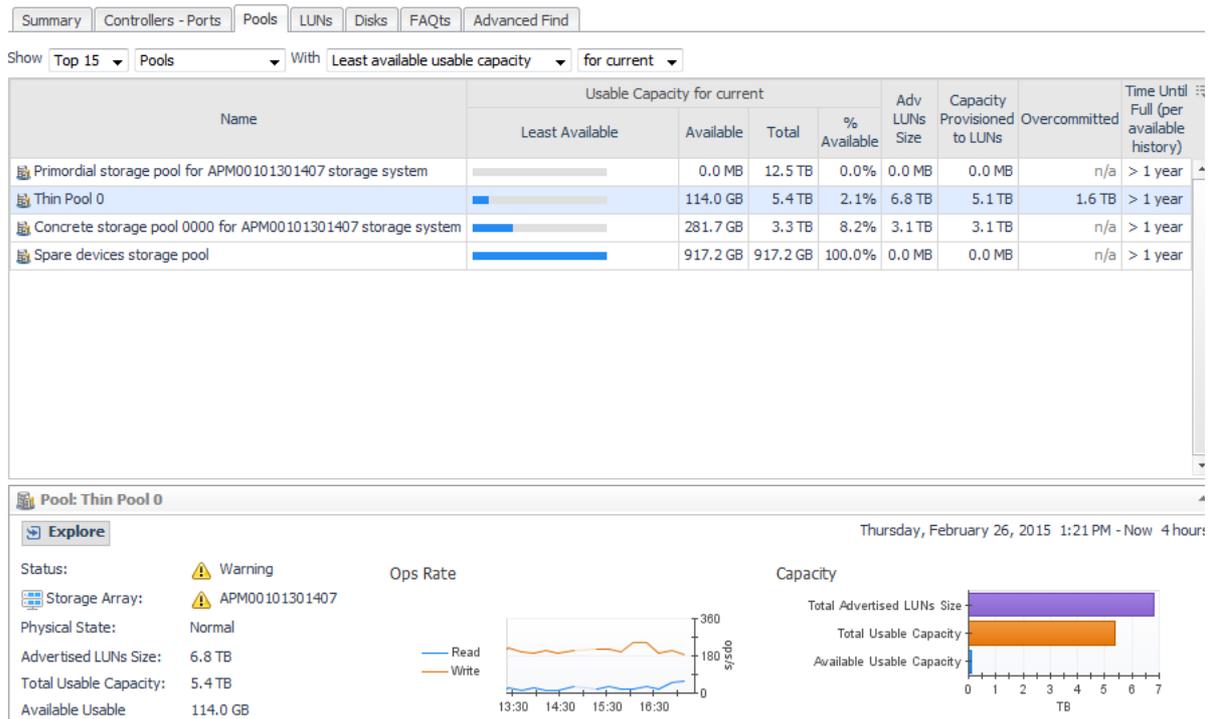
Connectivity and I/O Performance Monitoring

Foglight for Storage Management provides comprehensive topology views which detail all I/O paths and components on each I/O path from VMs down to their assigned physical storage devices. These views assist in determining where actual performance or connectivity problems are occurring during I/O requests, something which is not possible using traditional virtual infrastructure management tools. For more information, see Assessing Connectivity and I/O Performance.

Figure 3. Connectivity and I/O Performance Monitoring.
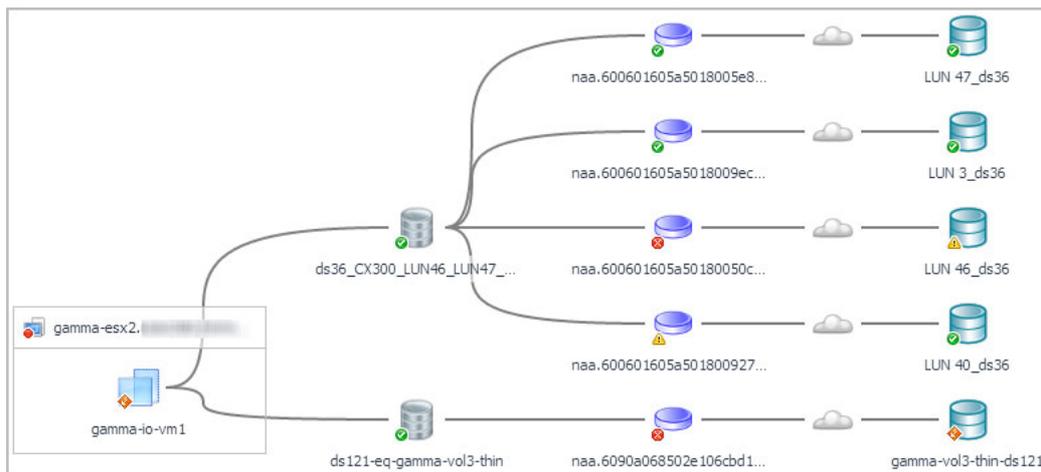
Navigating Foglight for Storage Management

Foglight for Storage Management is built on the Foglight platform. The following diagram and table introduce the common Foglight for Storage Management screen elements that are used in Foglight for Storage Management dashboards. If you need more information about how to use these elements, open the online help and navigate to **Foglight User Help > Getting Started > Working with Dashboards**.

Figure 4. Navigating Foglight for Storage Management.

Table 1. Screen Elements

Screen Element	Description
Navigation Panel	Contains a menu of all the dashboards that you can access based on your role. Select a dashboard to view in the display area. The panel operates like a drawer and can be open or closed using the arrow.
Display Area	Displays the contents of the selected dashboard.
Action Panel	Provides the following functions: • Lists the actions that you can perform on the current dashboard. • Lists the views and data that you can add to a new dashboard or report. • Provides access to context-sensitive help and the online help system. The panel operates like a drawer and can be open or closed.

Table 1. Screen Elements

Screen Element	Description
Breadcrumbs	Displays the path of dashboards you navigated to get to the current dashboard. Click a name in the path to return to that dashboard. **NOTE:** The browser Back button is disabled. Use the breadcrumbs to return to the previous screen.
Time Range	Controls the time period for the data displayed in the dashboard and any drill-down views you access. The default is the last four hours. Click the text to open the time range popup and set the range.
Sparkline	Shows the trend of a metric in a small space. The value beside the sparkline is the current value for the metric in the selected time range. When used in a table, sparklines provide an easy way to compare spikes or other trends in a group of metrics. Click a sparkline to plot all data points for the time period on a graph. **NOTE:** If the last collection failed for any reason, the sparkline value is *n/a*.
Status Icons	Displays the status of a storage resource. For more information, see Understanding Status, Alarms, and Rules in Foglight for Storage Management.

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 2. 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
Hitachi Data Systems	5988 (non-SSL) 5989 (SSL) Tuning Manager uses: 135 445 all ports above 1000	SMI-S query to the host running the Hitachi Command Suite or embedded SMI-S provider on VSP arrays. When running the Tuning Manager, the connection to the management host uses WMI (RPC).
HP EVA	5988 (non-SSL) 5989 (SSL)	SMI-S query to the host running Command View

Table 2. Network Port Requirements

Storage Device	Ports Used	Description
NetApp	80 443	DataOnTap API query to each filer
3PAR	5988 (non-SSL) 5989 (SSL)	SMI-S query to an embedded SMI-S provider on the array.

Sizing Your Monitored Environment

ℹ **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 3. 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.

ℹ **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 4. System Requirements

CPU	8-way 2.4 GHz CPUs — one of the following: • 2 quad core • 4 dual core • 8 single core
RAM	20 GB in total: • 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: • 20 GB for the Management Server • 100 GB for the Management Server Database Repository If using an embedded database repository: • Total of 140 GB on a RAID device available on the Management Server machine If using an external Database Repository: • 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 5. Management Server, Browser Interface, and Database Repository on a 64-bit Foglight-supported Platform

CPU	4-way 2.4 GHz CPUs — one of the following: • 1 quad core • 2 dual core • 4 single core
RAM	28 GB in total: • 16 GB for the Management Server • 8 GB for the Database Repository • 4 GB for the operating system
Storage	If using a built-in embedded Database Repository: • 220 GB, on a RAID device If using an external Database Repository: • For Management Server: 60 GB, on a RAID device • For Database Repository: 160 GB, on a RAID device

Table 6. Agent Manager on a 64-bit Windows or Linux Platform

CPU	4-way 2.4 GHz CPUs — one of the following: • 1 quad core • 2 dual core • 4 single core
RAM	6 GB in total: • 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 7. Test Environments

Operating System	Version	OS Architecture	Valid Installer
CentOS® Linux®	7.x	x86-64	*fglam-<ver>-linux-x86_64.bin*
Microsoft® Windows®	Server 2008	x86-64	*fglam-<ver>-windows-x86_64.exe*
	Server 2008RS Server 2012 Server 2012 R2	x86-64	*fglam-<ver>-windows-x86_64.exe*
Novell® SUSE Linux® Enterprise Server	11	x86-64	*fglam-<ver>-linux-x86_64.bin*
Red Hat® Enterprise Linux®	6.x	x86-64	*fglam-<ver>-linux-x86_64.bin*
Ubuntu® Linux	14.04.x LTS	x86-64	*fglam-<ver>-linux-x86_64.bin*

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 Foglight Evolve. When adding Foglight for Storage Management dashboard, 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 Foglight Evolve. When adding Foglight for Storage Management dashboard, 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.

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

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 8. Storage user roles.

Roles	Description
Storage Administrator	• Perform administrative tasks from the Storage Environment dashboard. *Excludes actions reserved for the Foglight for Storage Management Administrator role, such as creating and modifying agents, rules, and registry variables.* • View all Storage & SAN dashboards. • Create and manage Storage reports.
Storage QuickView User	• View all Storage & SAN dashboards. • Create and manage Storage reports.
Storage Report User	• 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**.

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 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
- 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 Appendix: Supported Storage Devices Table on page 182.
*   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.

    > **NOTE:**
    >
    > *   In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM to use this option. For more information, see Managing certificates on page 46.
    >
    > *   Storage agent only supports monitoring through IP address. Ensure that "Subject" or "Subject Alternative Name" field of the certificate includes the IP address of your device.

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 Appendix: Supported Storage Devices Table on page 182.
- 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 Appendix: Supported Storage Devices Table on page 182.
- 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 Processer (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 Appendix: Supported Storage Devices Table on page 182.

- 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.

i | **NOTE:**

- In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM to use this option. For more information, see Managing certificates on page 46.

- Storage agent only supports monitoring through IP address. Ensure that "Subject" or "Subject Alternative Name" field of the certificate includes the IP address of your device.

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 Appendix: Supported Storage Devices Table on page 182. 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.

i | **NOTE:**

- In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM to use this option. For more information, see Managing certificates on page 46.

- Storage agent only supports monitoring through IP address. Ensure that "Subject" or "Subject Alternative Name" field of the certificate includes the IP address of your device.

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 SMIs 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_StorageSyst
em",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 .

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 TestSMIProvider to verify if statistics logging is enabled for CLARiiON or VNX arrays.

To verify if statistics logging is enabled:

1   Log in to 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",Na
me="EMCBlockStatisticsService",SystemCreationClassName="Clar_StorageSystem",Sy
stemName="CLARiiON+APM001206012345
```

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

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

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

   ℹ | **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

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 refsys 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 Appendix: Supported Storage Devices Table on page 182.
- 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 and VPLEX metro version, see Appendix: Supported Storage Devices Table on page 182.
- The root account for a VPLEX array is required.

> **NOTE:**
> - In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM to use this option. For more information, see Managing certificates on page 46.
> - Storage agent only supports monitoring through IP address. Ensure that "Subject" or "Subject Alternative Name" field of the certificate includes the IP address of your device.

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 9. 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 Appendix: Supported Storage Devices Table on page 182.

    > **i** | **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
```

> **i** | **NOTE:**
>
> • In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM to use this option. For more information, see Managing certificates on page 46.
>
> • Storage agent only supports monitoring through IP address. Ensure that "Subject" or "Subject Alternative Name" field of the certificate includes the IP address of your device.

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
4000 Series	6000 Series
4100 Series	6100 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 Appendix: Supported Storage Devices Table on page 182.

- 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.

ⓘ | **NOTE:**

  - In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM to use this option. For more information, see Managing certificates on page 46.

  - Storage agent only supports monitoring through IP address. Ensure that "Subject" or "Subject Alternative Name" field of the certificate includes the IP address of your device.

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 HP 3PAR Arrays
- Configuring Agents to Monitor HP 3PAR 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.

ⓘ | **NOTE:**

  - In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM to use this option. For more information, see Managing certificates on page 46.

  - Storage agent only supports monitoring through IP address. Ensure that "Subject" or "Subject Alternative Name" field of the certificate includes the IP address of your device.

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 Appendix: Supported Storage Devices Table on page 182.

    *   For general access, the following permissions are required for the accounted 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 10. 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
fcp-adapter-get-iter	perf-object-counter-list-info	system-get-node-info-iter
fcp-adapter-list-info	perf-object-get-instances	system-get-ontapi-version
fcp-interface-get-iter	perf-object-get-instances-iter-end	system-get-version
fcp-node-get-name	perf-object-get-instances-iter-next	vfiler-list-info
fcp-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,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 11. 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
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
```

> **i** | **NOTE:**
>
> • In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM to use this option. For more information, see Managing certificates on page 46.
>
> • Storage agent only supports monitoring through IP address. Ensure that "Subject" or "Subject Alternative Name" field of the certificate includes the IP address of your device.

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.

Configuration Procedures

The preceding sections link to the folowing 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
- Managing certificates

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.

    > **i** | **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.
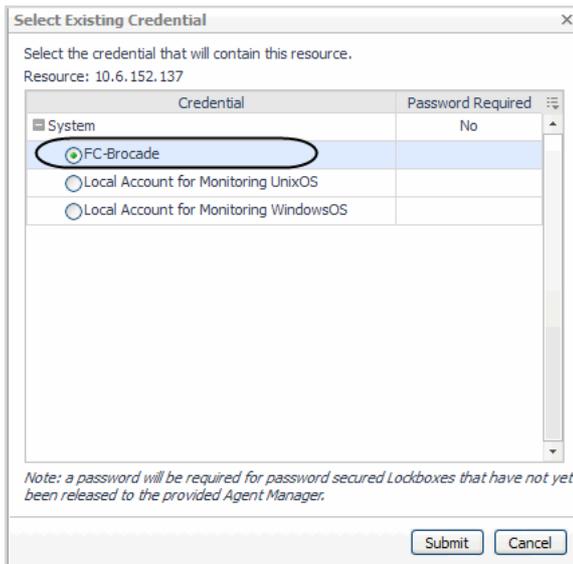
3   Click **Submit**.

   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 **Homes**, click **Storage Environment**.

2   Click the **Administration** tab.

3   Click **Configure SMIS Agent for Storage Device Monitoring**.

      The *Storage Device Setup* dialog opens.

4   In the *Add SMIS Storage Agent* section, select an agent manager host from the Agent Manager drop-down list.

5   In the *Add SMIS Storage Agent* section, configure the agent settings:

     a   In the *IP Address* field, type the IP address of the server hosting the agent manager.

     b   If the Agent uses a non-default (5988 or 5989) 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.

     c   Check the HTTPs check-box if the Agent uses SSL connection.

     d   Specify a name for the agent in the *Name* field (optional).

     e   Click **Add**.

6   Create or select a credential that contains the account information needed to access the storage device. For more information, see Assigning Credentials.

7   Click **OK** to exit the *Storage Device Setup* dialog.

Managing certificates

Syntax Conventions

In order to successfully make use of the Foglight commands in your monitoring environment, review the syntax conventions before getting started. The syntax conventions are as follows:

- Generic examples follow the UNIX path structure that uses forward slashes '/' to separate directories.

- Platform-specific examples follow standard platform conventions. For example, UNIX-specific examples use forward slashes '/' as directory delimiters, while Windows examples use backslashes '\'.

- *<foglight_home>* is a placeholder that represents the path to the Foglight Management Server installation.

- *<foglight_agent_mgr_home>* is a placeholder that represents the path to the Foglight Agent Manager installation. This can be the location of the Foglight Agent Manager installation on a monitored host, or the

home directory of the Foglight Agent Manager that comes embedded with the Foglight Management Server. For example:

Path to the Foglight Agent Manager installation on a monitored host (Windows):

C:\Quest\Foglight_Agent_Manager

Path to the embedded Foglight Agent Manager installation (Windows):

C:\Quest\Foglight\fglam

• Unless otherwise specified, Foglight commands are case-sensitive.

Managing certificates for FglAM

Foglight Evolve agents use Foglight Agent Manager (FglAM) to manage certificates for SSL encryption connection.

Prerequisite

All the certificate-related command line options require that FglAM be **up and running**.

Add a certificate

```
bin/fglam --add-certificate "user alias 1"=/path/to/certificate/file
```

• Validate the certificate and ensure the following:

  ▪ It is not expired.

  ▪ It is an X.509 format.

  ▪ FglAM requires the Base64 format. To verify if the certificate file is encoded with Base64, open the certificate with a notepad and the certificate should be similar to the following example:
    ```
    -----BEGIN CERTIFICATE-----
    XXXXXXXX=
    -----END CERTIFICATE-----
    ```

    > **i** | **NOTE:** If the certificate is not Base64 format, use openssl command to convert the certificate file into a Base64 file. Use either of the following commands depending on the source form:
    > ```
    > openssl x509 -inform DER -in xxx.cer -out xxx.crt
    > ```
    > or
    > ```
    > openssl x509 -inform PEM -in xxx.cer -out xxx.crt
    > ```

• The `alias` is required and is used in the list and delete operations to refer to the certificate. It can be anything.

List installed certificates

```
bin/fglam --list-certificates
```

Print out a list of certificates and the aliases that refer to them.

Refer to the example output below:

```
List of installed certificates:

  Alias              Certificate Info

  -----              ----------------

  user alias 1       XXXX
```

Delete a certificate

Remove a certificate referred to by an `alias`.

```
bin/fglam --delete-certificate "user alias 1"
```

A full example for managing certificate for FglAM

- Add an example certificate into FglAM certificate store

```
C:\Quest\Foglight\fglam\bin>fglam.exe --add-certificate "Evolve-test"="D:/Evolve-
test.crt"

…

2020-02-27 16:31:01.000 INFO  [native] Certificate added: Certificate from
  D:\Evolve-test.crt added as Evolve-test
```

- List the example certificate in the FglAM certificate store

```
C:\Quest\Foglight\fglam\bin>fglam.exe --list-certificate

…

  Alias                      Certificate
  -----                      -----------
  Evolve-test                    Issuer:
                               CN: XXX
```

- Delete the example certificate from the FglAM certificate store

```
C:\Quest\Foglight\fglam\bin>fglam.exe --delete-certificate "Evolve-test"

…

2020-02-27 16:28:21.000 INFO  [native] Certificate deleted: Certificate
  Evolve-test deleted
```

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 5. Storage Collector Agents view

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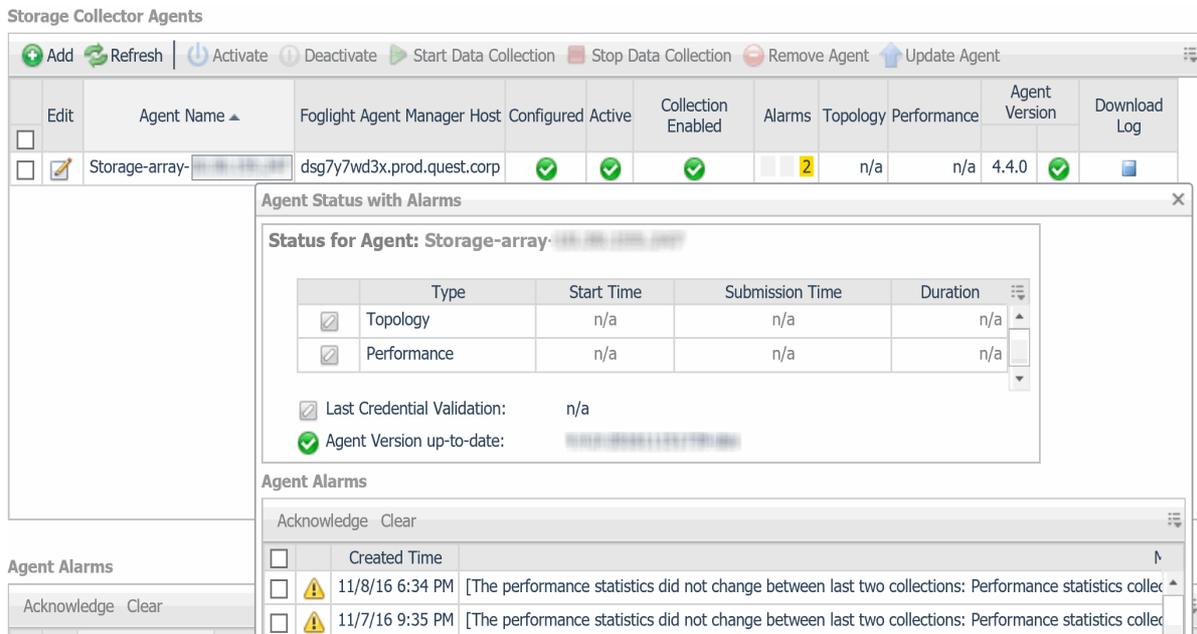
From this table you can select an alarm to view the alarm details.

To view alarm details or administer alarms:

1   Click on the required alarm.
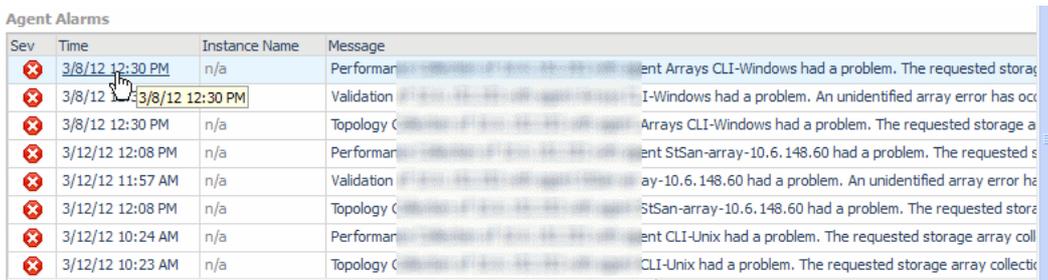
The alarm message box opens.

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 6. Edit Agent Properties
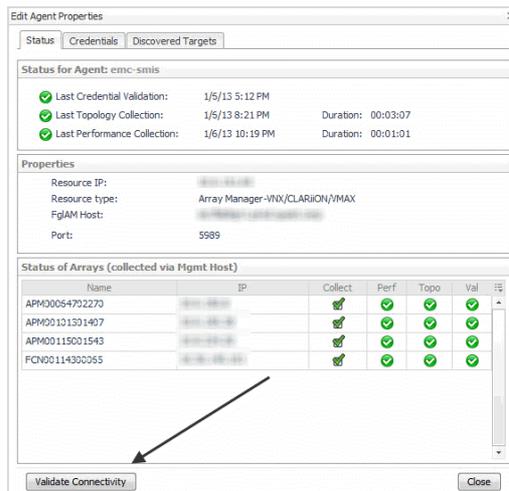
Properties Panel

The Properties view varies based upon the agent type.

Port Property

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

Figure 7. Port Property
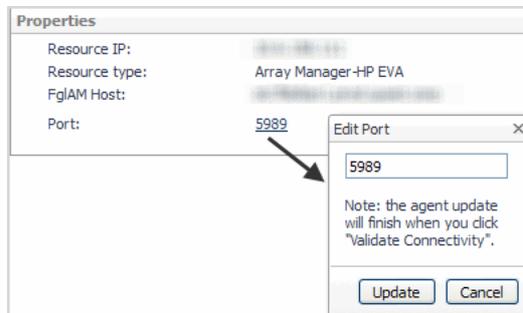
To change the port:

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 8. Path Property
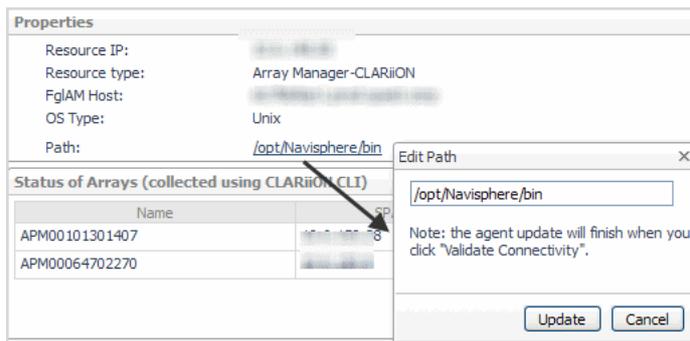
To change the path:

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 9. Credential Validation Status
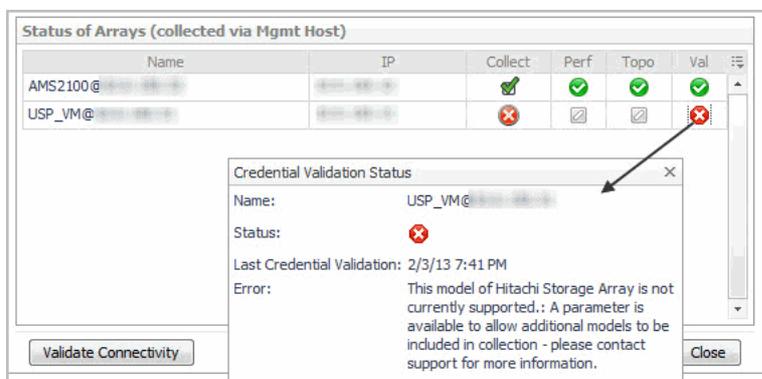
Managing Credentials

This tab displays the credentials for the selected agent.

Figure 10. Managing Credentials
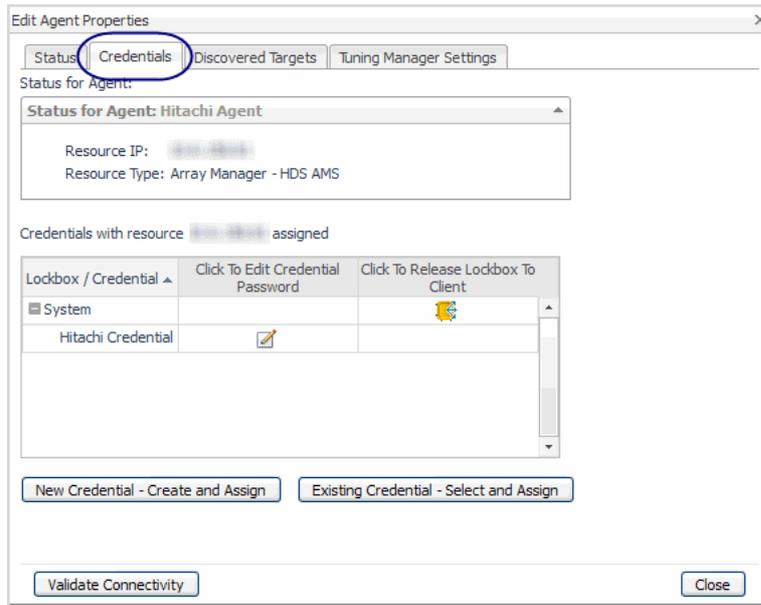
From this tab you can create or select credentials. For procedures, see Assigning Credentials. You can also edit the password for a credential.

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.
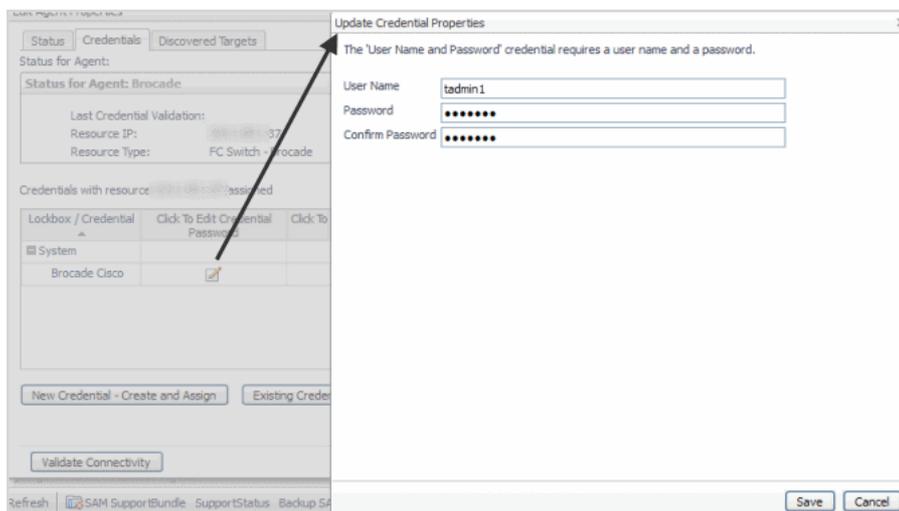
2   Modify the credentials as required.

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.
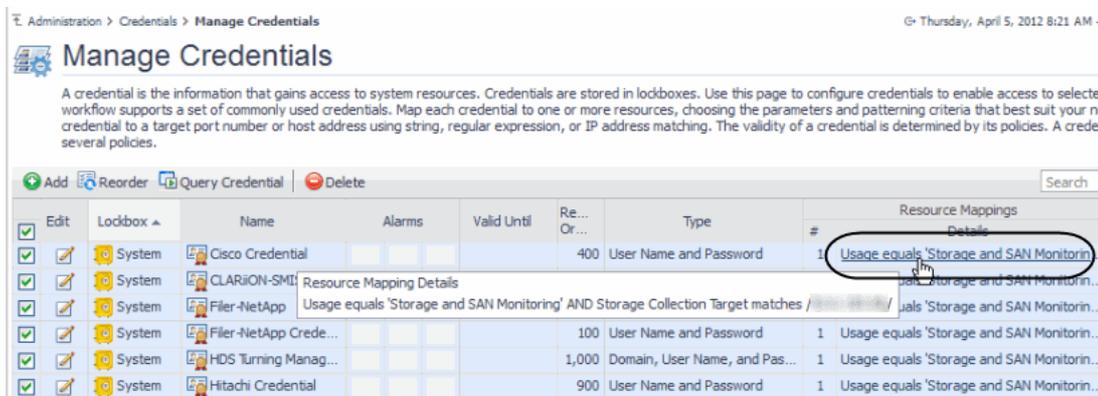
The Update Resource Mapping of Credential page opens.

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 11. Discovered Targets tab
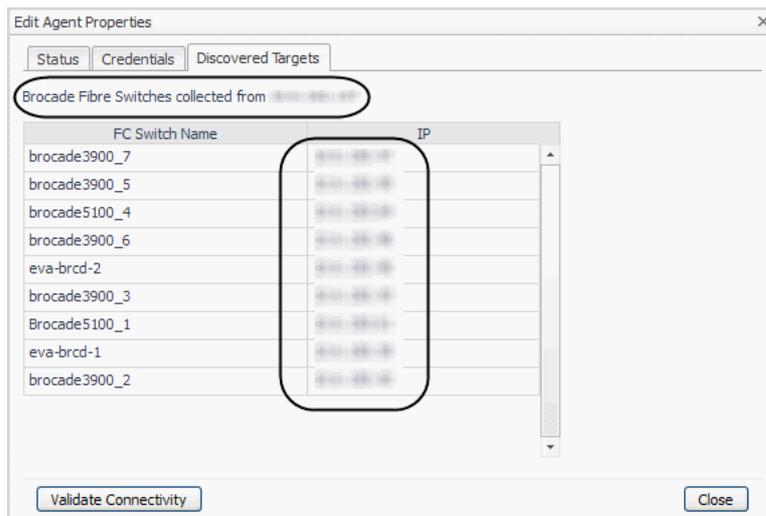
Arrays Discovered Targets Tab

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

Figure 12. Arrays Discovered Targets tab
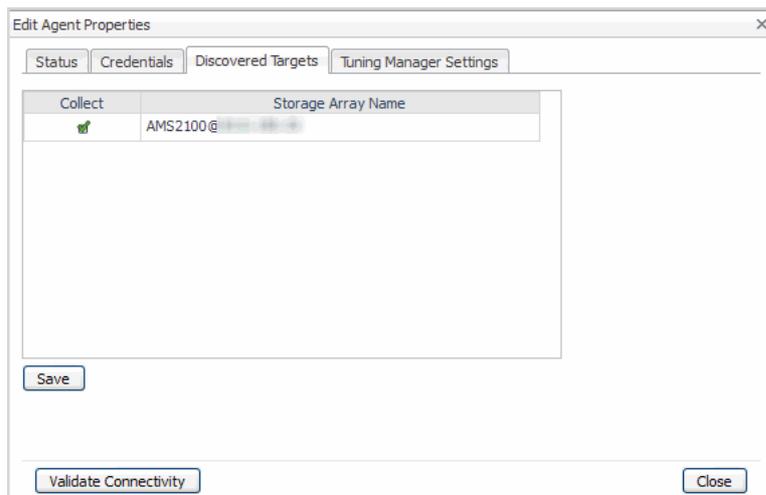
The following procedures allow you to disable/enable arrays from being monitored.

Disable/Enable Array Targets

1   Click the storage array name so the corresponding icon is checked or cleared, and click **Save**.
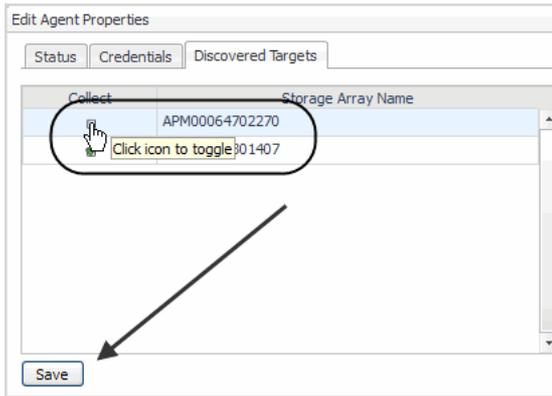
The Saving message box displays error messages.

2 Click **OK**.

The properties are saved.

Managing CLARiiON 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 CLARiiON CX Series Arrays (CLI).

Figure 13. Array Details
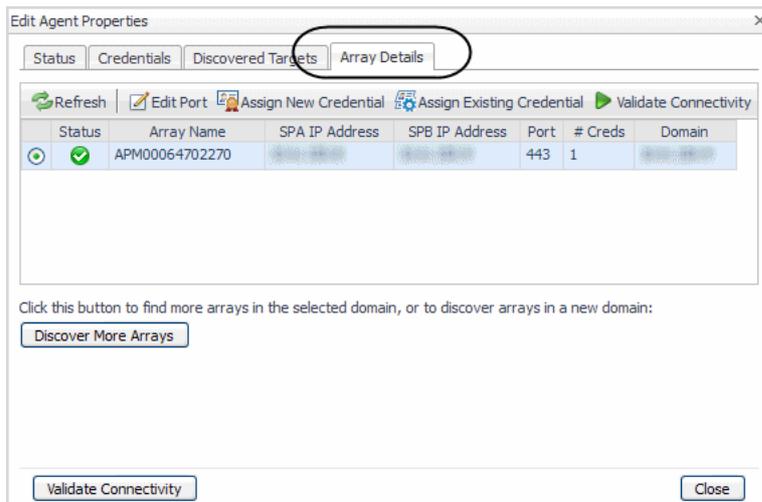
Managing the Hitachi Tuning Manager

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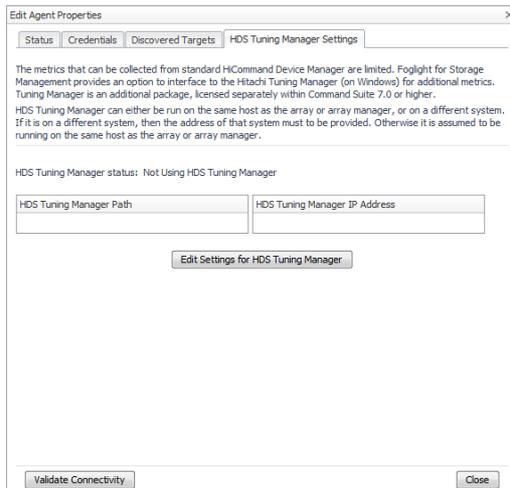
From this tab you can edit settings for the HDS Tuning Manager.

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).
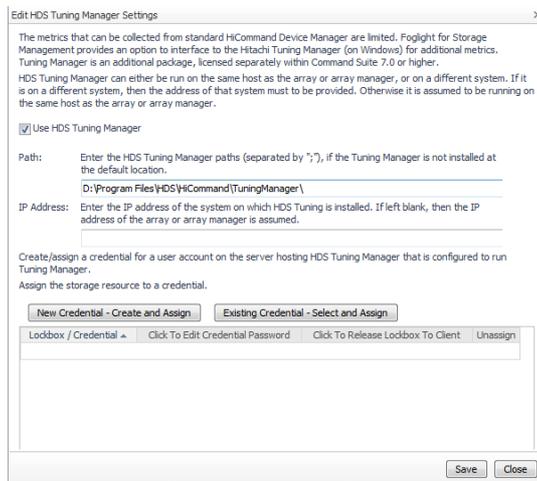
3   Create a new credential or assign an existing credential to access the Tuning Manager. For help on this task, see Assigning Credentials.

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.

Storage Environment

Your Trial

| Monitoring | FAQts | Reports | Storage Capacity | Administration | Getting Started |

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 an
- Configure Duplicate

Storage Collector Agents

Add Refresh | Activate Deactivate Start Data Collection Stop Data Collection Remove Agent Update Agent

	Edit	Agent Name ▲	Foglight Agent Manager Host	Configured	Active	Collection Enabled	Alarms	Topology
☐	📝	AMS-USP	delta-fms-vm4.vfs.stc.us.qsft	✅	✅	✅	n/a	n
☐	📝	Brocade	delta-fms-vm4.vfs.stc.us.qsft	✅	✅	✅	n/a	11/9/16 3:55 F
☐	📝	Cisco-mds0148-1	delta-fms-vm4.vfs-stc-us-qsft	✅	✅	✅	n/a	n

Using Foglight for Storage Management

This section tells you how to verify that Foglight for Storage Management is capturing storage collection data for all the devices you are interested in monitoring.

This section covers the following topics:

- Verifying StorageCollector/Generic SMIS Storage Agents are Collecting Storage Data
- Understanding Metric Data in Charts and Tables
- Modifying and Extending Data Collection
- Next Steps

# Verifying StorageCollector/Generic SMIS Storage Agents are Collecting Storage Data

To begin, review the Foglight for Storage Management dashboards to verify you are monitoring the devices you want to monitor. You need the IP address of the Foglight for Storage Management Management Server and your user credentials from the person who installed and configured Foglight for Storage Management.

ℹ️ | **NOTE:** This procedure is intended for Foglight for Storage Management users with the roles of *Storage Administrator*, *VMware Administrator,* and *Hyper-V Administrator*.

To log in and confirm the list of monitored devices:

1 Open a supported browser. For a list of supported browsers, see the *System Requirements Guide*.

2 In the navigation bar, type the IP address followed by the port number 8080. For example:

```
http://<Foglight for Storage Management_Management_Server_IP_Address>:8080
```

3 Log in to Foglight for Storage Management using your user credentials.

4 On the navigation panel, expand **Dashboards**.

These menu items are of particular interest for monitoring storage performance: **Storage & SAN**, **VMware**, **Hyper-V**, and **Infrastructure**.

5 Expand **Storage & SAN**.

The following menu items are available:

- Storage Capacity — Monitor your storage capacity by device type.
- Storage Environment — Monitor storage devices in your storage environment.
- Storage Explorer — Find and examine any storage device in your storage environment.

6   Click **Storage Environment**.

7   Ensure the **Monitoring** tab is selected.

8   Click the top half of each active tile and review the list of devices in the quick view.
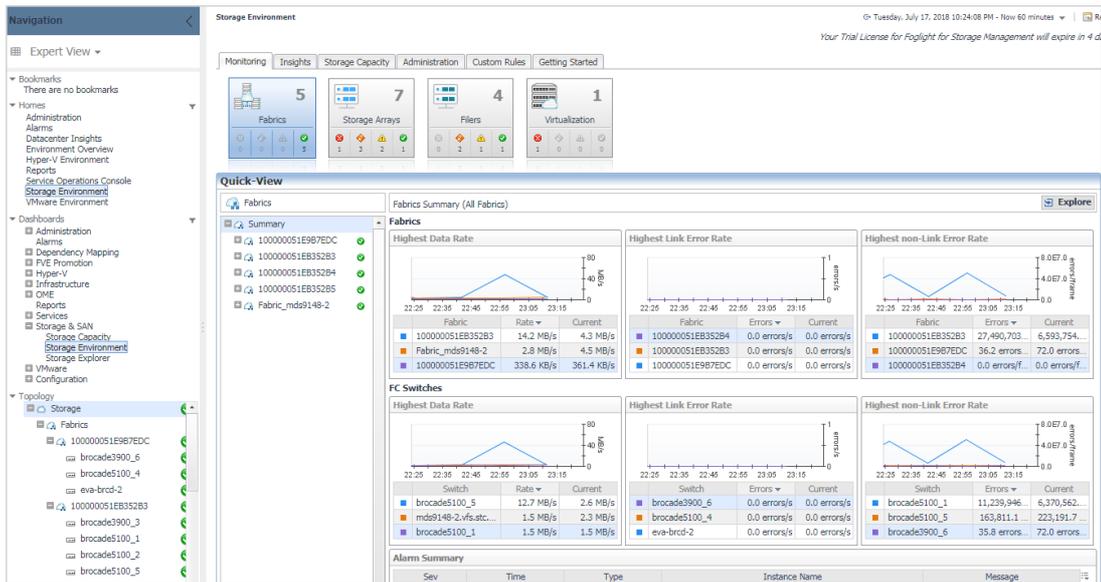
9   If you do not see a storage device that you think should be monitored, review the list of configured Storage Collector agents.

   f   On the **Storage Environment** dashboard, click the **Administration** tab.

   > **i** | **TIP:** If you do not see the **Administration** tab, ask your Foglight for Storage Management Administrator to add the role *Storage Administrator* to your user account.

   g   In the *Storage Agents > StorageCollector Agents* list, look for the Storage Collector agent that monitors the missing device or device type. When an agent monitors a device type, click the **Edit** icon to view a list of named devices in the **Edit Agent Properties** dialog box.

   Or

   In the *Storage Agents > Generic SMIS Storage Agents* list, look for the SMIS Storage agent that monitors the missing device or device type. When an agent monitors a device type, click the **Edit** icon to view a list of named devices in the **Edit Agent Properties** dialog box.

   h   If a StorageCollector agent or Generic SMIS Storage agent does not exist for a device, or if the agent exists but it is disabled or its data collection is turned off, contact your Foglight for Storage Management Administrator. For instructions about agent tasks, see the *Foglight for Storage Management Installation Guide*.

10 Go to the dashboard for the storage device or switch and ensure that both performance and topology information have been submitted recently.

Collecting Storage Data for Virtualized Devices and Servers

To collect storage data for virtualized devices and servers:

1 On the navigation panel, expand the dashboard menu for your virtualization software. For example, either VMware or Hyper-V.

> **i** | **TIP:** If you do not see the VMware or Hyper-V menu, ask your Foglight for Storage Management Administrator to add the appropriate administrator role to your user account.

2 To verify the virtualization agents:

a Click the Hyper-V or VMware **Explorer**.

The Explorer opens a Virtual Infrastructure Topology tree—displayed in the navigation panel below the list of Dashboards—that contains branches for each monitored vCenter or Hyper-V server. For detailed information about the dashboards available through this tool, see the *Managing Virtualized Environments User and Reference Guide*.
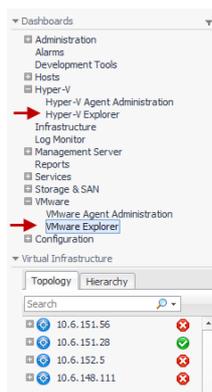
b If the Virtual Infrastructure Topology list is empty, your Foglight for Storage Management Administrator needs to create a Performance agent to monitor at least one vCenter or Hyper-V server. For instructions, see the Foglight for Storage Management Installation Guide.

c If the list is not empty, expand the tree and select a virtualization host or server.
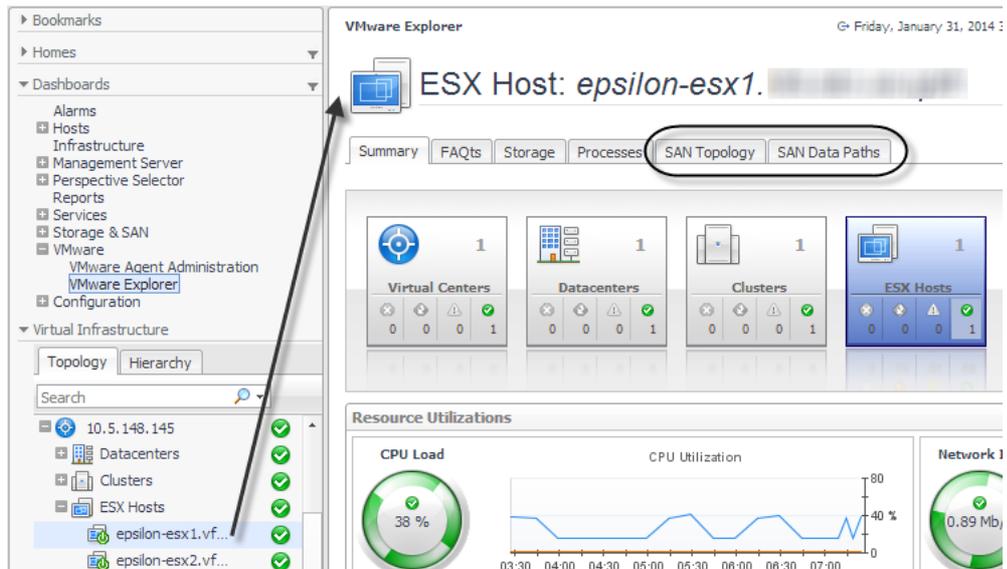
d   Click the **SAN Topology** tab.

e   Verify that you can see the storage-side of the virtual infrastructure, identified by the icons that are circled in the following diagram. If these elements are missing, the Performance agent monitoring this host is not collecting the data necessary to make connections to storage and SAN data. To enable storage data collection, see Collecting Virtual Storage-to-SAN Relationships.
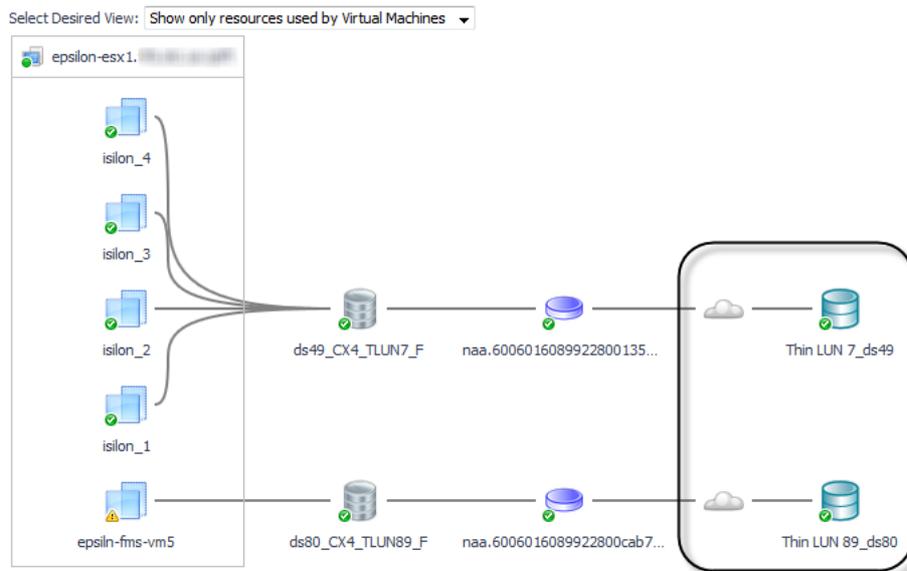
After you finish with Performance agents, review monitored hosts.

3   On the navigation panel, click **Infrastructure**.

a   In the Select a Service box, select **All Hosts**.

The tiles organize physical hosts by their operating system.

b   Click the **Inferred** tile.

The Inferred tile lists physical hosts that Foglight for Storage Management has inferred based on an analysis of the switch, array, and filer ports it is monitoring (a process called *dependency processing*). When physical hosts are connected to storage devices, you can drill down on a host and view connections in SAN Topology tabs.
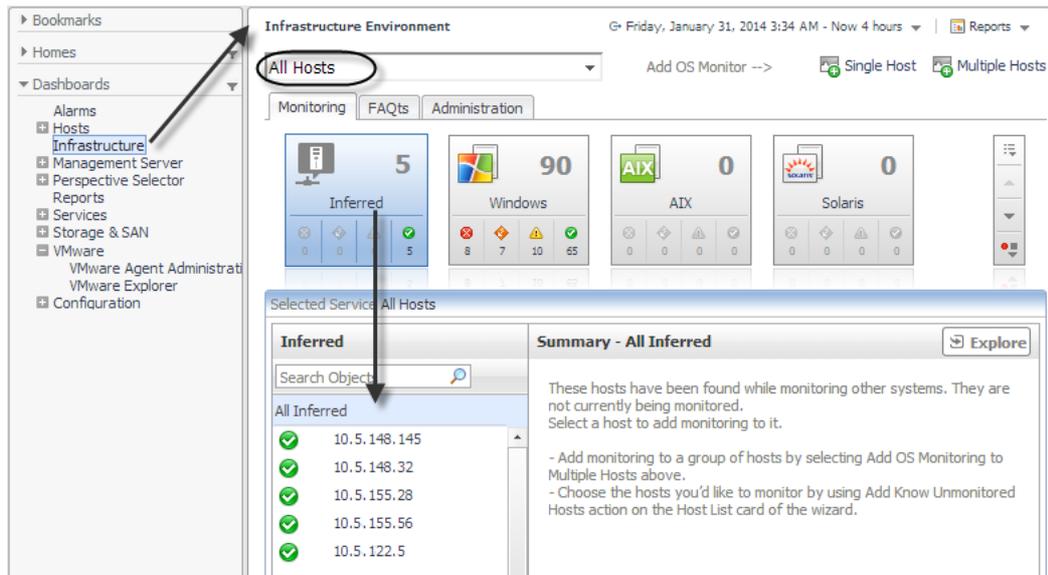
    c   If the Inferred tile does not show any inferred hosts, you may want to enable dependency processing to begin collecting the names of inferred hosts. For more information, see Inferring Physical-Host-to-Storage Relationships.

You have finished verifying that agents are collecting data.

Understanding Metric Data in Charts and Tables

In the Storage & SAN dashboards, charts and tables display metric data. Data is collected by Storage Collector agents, aggregated into collections, and the collections are published to the SAN & Storage dashboards at regular intervals. For more information about storage collection schedules and the type of data collected, see Modifying Data Collection Schedules.

The data displayed in charts and tables represents data for one or more intervals in the selected time range as follows:

- **Current**. The value collected in the last interval in the selected time range. In charts, the last plotted value is the current value.

- **Period**. Aggregated values for the entire selected time range. Period values are often used to provide context for current values.

- **Historical**. Individual values for each collection interval in the selected time period. Historical values are often presented as datapoints in a plot chart or as sparklines to show how metrics changed over the time period.

- **Latest**. Values in the latest collection interval available, *irrespective of the selected time range*. If data collection is enabled, this value reflects the latest collection. If data collection is disabled, this value represents the last collection made by the agent. Although latest values are tracked, the SAN & Storage dashboards do not display these values.

For indepth information about metrics, see http://communities.quest.com/docs/DOC-12862.

Values are not available (*n/a*) under the following circumstances:

- The device vendor does not provide the necessary metric. In this case, the text *n/p by vendor* appears after the metric name in column headings.

- A device is *offline* (reported in the State field).

- A device is not actively being used, such as when a disk is configured as a spare (reported in the Used or Role fields).

- For the Latency metric (which is a partially computed metric), when the operations/second value is very low, the latency metric may not be submitted during a collection interval.

- If all other situations do not apply, then it is likely that data collection failed for some reason. If the current value is unavailable for a time range that occurs in the past, you can try changing the selected time range to end before or after the problem interval.

Modifying and Extending Data Collection

You can modify and extend data collection in the following ways. You may want to make these changes now, or adjust the settings in the future if you find a need.

Table 13. Data collection options

Options	Instructions
If not already enabled during installation, collect data about virtualization device-to-SAN relationships and display this information in SAN topology diagrams. Requires a VMware or Hyper-V Performance agent.	Collecting Virtual Storage-to-SAN Relationships
Infer connections from physical hosts to storage and show the connections in topology diagrams.	Inferring Physical-Host-to-Storage Relationships
Change the default collection interval.	Modifying Data Collection Schedules
Modify when rules trigger alarms (change threshold values) and add a list of email addresses to notify when alarms occur.	Managing Foglight for Storage Management Rules

Next Steps

Your next steps depend on whether you want to monitor your storage environment to identify problems or whether you need to respond to the report of a problem in the virtual infrastructure.

Monitoring Your Storage Environment

The following workflow suggests one approach to monitoring your storage environment and investigating issues. You may prefer a different approach, depending on your monitoring needs.

1 **Performance Monitoring** — Start by assessing alarms on all storage devices. See Monitoring Storage Performance.

2 **Capacity Monitoring** — After you acknowledge and/or resolve device-level alarms, you may want to investigate individual storage devices and their components. See Investigating Storage Devices.

3 **Connectivity and I/O Performance Monitoring** — You can identify performance or connectivity problems that occur during I/O requests by viewing diagrams that place storage components within the context of the virtualization environment, from VMs and hosts to storage devices. See Assessing Connectivity and I/O Performance.

Responding to Problem Reports

Storage Administrators need to respond to reports about problems in the storage environment.

- When you receive reports from colleagues about poorly-performing VMware virtual machines, use the Storage Troubleshooting analysis tool to determine whether resources in the SAN are contributing to the problem. For instructions, see Troubleshooting Storage Performance.

- When you receive emails from Foglight for Storage Management about a storage device or component that has entered a problem state, click the link in the email to navigate to the dashboard that provides details about the alarm. To learn how to set up email notifications, see Configuring Email Notifications for Alarms.

Monitoring Storage Performance

This section introduces the Storage Environment dashboard and guides you through monitoring your storage environment by assessing device status and alarms. The next sections provide alternative approaches to assessing your storage environment through the use of questions or by assessing the connectivity and port performance within the context of your virtual infrastructure. The last section introduces reports.

This section covers the following topics:

- Introducing the Storage Environment Dashboard

- Monitoring Your Storage Environment

- Asking Questions About the Monitored Storage Environment

- Assessing Connectivity and I/O Performance

- Monitoring Storage Capacity

- Creating Storage Reports

Introducing the Storage Environment Dashboard

The starting point for monitoring storage performance is the Storage Environment dashboard. The Storage Environment dashboard contains the following tabs:

- **Monitoring Tab** — Monitor your overall storage environment by device type. For more information, see Summary and Resource Information for each Collected Target:.

- **Insights Tab** — Break down to three views, *Analytics*, *Live Troubleshooter*, and *Reports*, to:
    - Retrieve important data about your monitored storage environment. For more information, see Asking Questions About the Monitored Storage Environment on page 80.
    - Investigate a potential storage performance issue. For more information, see Starting a Troubleshooting Investigation on page 148.
    - Use templates to create reports on your storage environment. For more information, see Creating Storage Reports on page 94.

- **Storage Capacity** tab — Monitor your storage capacity by device type. For more information, see Monitoring Storage Capacity.

If your Foglight for Storage Management user account includes the *Storage Administrator* role, the Storage Environment dashboard also displays these tabs:

- **Administration Tab** — Manage configured agents, credentials, and modify data collection settings.

- **Getting Started Tab** — Purchase a product license.

To open the Storage Environment dashboard:

- On the navigation panel, under Dashboards, click **Storage & SAN** > **Storage Environment**.

The first time you open this dashboard, the Monitoring tab is displayed, showing the overall status of your monitored storage environment.
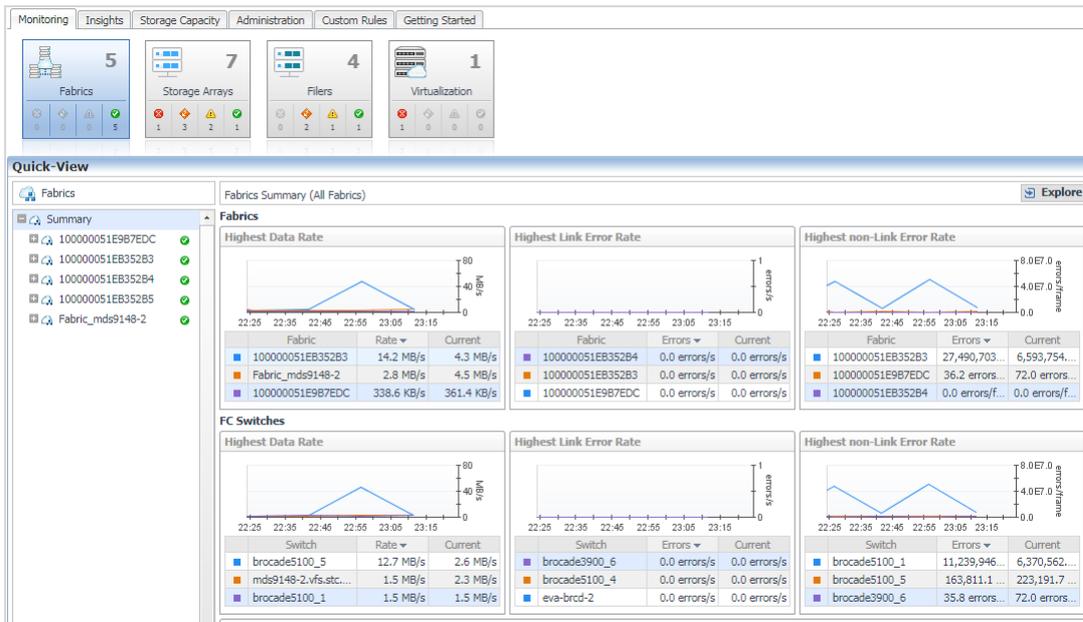

Table 14. The Monitoring tab contains the following screen elements:

Screen Element	Description
Time Range	Controls the period of time represented in the dashboard. The default is the last four hours. For more information, see "Time Range" in the online help.
Tiles	Summarizes how many of each type of device—Fabrics, Storage Arrays, and Filers—are being monitored, and breaks down the total number by alarm severity (from left to right: Fatal, Critical, Warning, and Normal). Tiles control the Quick View area as follows: • Click the top half of a tile to open the device type's quick view with the Summary view displayed. • Click a status icon in one of the tiles to open the device type's quick view containing only devices with that status.
Quick View	Contains four areas: Device List, Device Summary, FAQts, and Alarm Summary.
Device List	Displays the list of storage devices that match the selected tile. • Click *Summary* to display the top storage devices in terms of key performance or capacity metrics. • Click a device name to display metrics for that device only.
Device Summary	Displays performance and capacity metrics for the device selected in the Device List.
FAQts	Offers common searches in the form of questions. Scroll through questions, and click **Show Me** to see the answer to the currently displayed question. For more information, see Asking Questions About the Monitored Storage Environment.
Alarm Summary	Displays a list of alarms for the device selected in the Device List. For more information, see Understanding Status, Alarms, and Rules in Foglight for Storage Management.

Summary and Resource Information for each Collected Target:

1 Open the navigation panel, under **Dashboards**, select a target type. Then, select a target and click **Explore**.

2   In this view, you will see the following items:

- **Product Name:** Shows the target type name

- **Vendor:** Shows vendor name

- **Model:** Shows the model of the target

- **DeviceID:** Shows the name of the target

- **IP Address:** Shows the IP addresses of the target

- **Total Disk Capacity:** Shows the total disk capacity of the target

- **Missing or Removed Disks:** Shows the missing or Removed Disks, if any

- **Disks with no Information:** Shows the disks reported as No Information, if any

Monitoring Your Storage Environment

When you begin monitoring your storage environment, a good way to start is by identifying poorly-performing devices and resolving the issues that are contributing to the problems. In Foglight for Storage Management, all storage devices and their child components are assigned a status, which enables you to see at glance which elements in your storage infrastructure need attention. Any device that enters a non-Normal status triggers an alarm. For more information, see Understanding Status, Alarms, and Rules in Foglight for Storage Management.

The procedures in this section show you how to use the Monitoring tab in the Storage Environment dashboard to assess alarms and drill down to the components used by storage devices, such as the LUNs and NASVolumes that supply the physical storage for datastores.

This section describes the following topics:

- Understanding Status, Alarms, and Rules in Foglight for Storage Management

- Reviewing the Status of All Devices

- Assessing Storage Alarms

- Monitoring Fabrics

- Monitoring Storage Arrays

- Monitoring Filers

Understanding Status, Alarms, and Rules in Foglight for Storage Management

In Foglight for Storage Management, all storage devices and their child components are assigned a status, which enables you to see at a glance which entities in your storage infrastructure need attention. Status and alarms are controlled by rules that can be based on data, time, schedules, or events. The rule conditions define which values reflect acceptable behavior (Normal status) and which values warrant an alarm (Warning, Critical, or Fatal status). As the value associated with a monitored entity passes a condition threshold, Foglight for Storage Management generates an alarm and changes the entity's status accordingly.

i | **NOTE:** When a component is selected, its detail views display the component's Status followed by its State. *Status* is determined by Foglight for Storage Management as describe above. *State* refers to the physical state of a component as reported by the vendor; if the vendor does not provide the physical state, the state is *unknown*. A component's physical state may affect its status only when an enabled rule triggers alarms based on state. Consult with your Foglight Administrator if you want to enable or create rules that perform this check.

A storage device often has large numbers (thousands) of child components. With a few exceptions, alarms on child components do *not* change the status of the parent device. For example, a failed disk may have a Fatal status, but because arrays are designed to cope with a failed disk, the parent device continues to display a Normal status. The parent device status may be changed by child components in the following circumstances:

- Controller problems typically affect the performance of the storage array or filer, so the parent device inherits the alarm status of the controller. Pool alarms reflect capacity issues and performance problems that can affect many users of the storage array or filer, so the parent device inherits the alarm status of the pool or aggregate.

- When a significant percentage of child components have problems (for example, many disks are failing), the problems may be indicative of a systemic problem. In this case, the parent device status changes when the number of affected child components reaches a threshold defined in rules.

For information about changing default rules and alarm settings, see Managing Foglight for Storage Management Rules.

Reviewing the Status of All Devices

Use the Monitoring tab in the Storage Environment dashboard to gain a high-level understanding of the status of the devices in your environment, organized by device type. For a general description of the dashboard, see Introducing the Storage Environment Dashboard.

***To monitor the storage environment:***

1   On the navigation panel, under Dashboards, click **Storage & SAN** > **Storage Environment**.

2   Click the **Monitoring** tab.

The time range and selected tile are the same as the last time the dashboard was opened.

Optional—Change the Time Range. For an initial review, use the default time range.

3   Scan the lower part of the tiles.

4   If any of the tiles show that there are devices with the ❌ Fatal, ◆ Critical, or ⚠ Warning status, do one of the following:

- To view all levels of alarms, click the top part of a tile that has the highest number of devices with the most severe errors. Go to the next section, Assessing Storage Alarms.

- To view alarms at one severity level only, such as all Critical alarms, click the Critical status count. Go to the next section, Assessing Storage Alarms.

5   If all tiles report that devices are in the Normal status, it means that the devices are operating within acceptable parameters. The next step is to review the devices to see if any of their child components show an alarm status. See one of the following topics:

- Monitoring Fabrics
- Monitoring Storage Arrays

- Monitoring Filers

Assessing Storage Alarms

When a storage device or component enters an unacceptable state (as defined in a rule), the rule that monitors the entity triggers an alarm and sets the status of the resource. Examine the alarm messages starting with the most severe alarms.

This walkthrough assumes that you are looking at alarms of all severity levels in an Alarm Summary view. In many places in the software you can restrict your assessment to resources with the same alarm severity. This can be useful when you want to prioritize your alarm assessment, such as focusing on all storage arrays with Critical alarms first, and then on the Warning alarms.

To assess alarms:

1   In the Alarm Summary view, review the alarm messages to understand the issues. If the list contains multiple levels of alarm severity, start with the highest severity alarm.


> **i** | **TIP:** If you see alarms on devices or components that you think are operating within acceptable parameters, consider creating new rules to better suit your environment. For more information, see Managing Foglight for Storage Management Rules.

2   If you need more details to understand the issue, click the alarm message.

An Alarm window displays more information about the alarm and troubleshooting tips.

> **i** | **TIP:** To bypass the Alarm window and go straight to the Choose Diagnostic Focus Time window (described in the next step), click an instance name instead of the message.
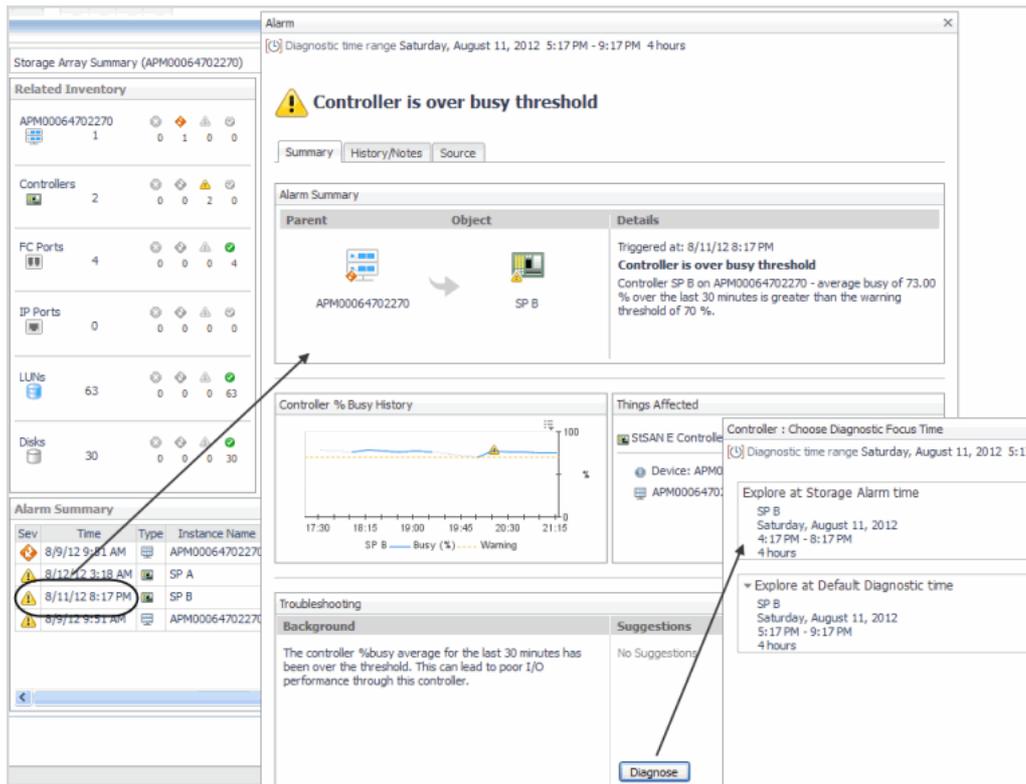
3 From the Troubleshooting pane, click the **Diagnose** button.

4 Choose the time period to use as your diagnostic time range:

- **Explore at Storage Alarm time**. Select this option when you want to view diagrams and other details of the affected component at the time the alarm occurred. Shows data for the time period leading up to and including the alarm time. For example, given an alarm time of 10:32 AM and the default four hour time range, the diagnostic time range is set to 6:32 AM – 10:32 AM.

- **Explore at Default Diagnostic time**. Select this option when you want to determine if the situation causing the alarm persisted or if it resolved on its own. Shows data before and after the alarm, with the alarm time positioned three quarters of the way into the time range. For example, given an alarm time of 10:32 AM and the default four hour time range, the diagnostic time range is set to three hours before the alarm and one hour after the alarm, that is, 7:32 AM – 11:32 AM. If the current time falls within the range, for example, it is currently 11:05 AM, the time range is set to 7:32 AM – 11:05 AM.

A component dashboard opens with its time range set to the selected diagnostic time range.

5 Review the component dashboard to better understand the data that led to the alarm. If you navigate to other dashboards, the diagnostic time range remains the same.

6 When you complete your investigation, in the breadcrumbs, click **Storage Environment** to return to the Choose Diagnostic Focus Time window. If desired, choose the other diagnostic time range.

7 When you are finished, close the Choose Diagnostic Focus Time window, and in the Alarm window click one of the following options:

- **Acknowledge**. Continues to display the alarm, but it is marked as acknowledged until the alarm is triggered again. For example, for Warnings, an appropriate action may be to acknowledge the alarm and ignore it.

- **Acknowledge Until Normal**. Continues to display the alarm, but it is marked as acknowledged until the affected component returns to the Normal status. This is useful when a component has failed and you want to know when it is replaced.

- **Clear**. Deletes the alarm. Choose this option when the situation is resolved.

8   Close the Alarm window.

>   **TIP:** When you close the window, the time range returns to the time range in use before your alarm
>   analysis. If it does not, in the Time Range either click the **Frozen Time Range** [⟳] icon to return to
>   real time or click the arrow to expand the zonar and set the range. For more information, see
>   "Working in a Current or a Diagnostic Time Range" in the online help.

9   Take action to resolve the issue in your storage infrastructure, either by yourself or by notifying the
     appropriate person.

Monitoring Fabrics

Foglight for Storage Management provides insight into both physical and virtual fabrics available with Brocade and
Cisco Fibre Channel (FC) switches. A physical fabric is a group of interconnected FC switches. The definition of a
virtual fabric differs depending on the vendor:

*   Brocade switches enable customers to group ports on physical switches into logical switches. Logical
     switches and physical switches can then be interconnected into virtual fabrics. Brocade creates logical ISL
     ports to interconnect logical switches. No metrics are available for LISL ports.

*   Cisco switches enable customers to create virtual storage area networks (VSANs) partitioned from a
     physical fabric. A VSAN is a logical group of ports, where the ports are located on one or more of the
     interconnected FC switches that form the physical fabric.

Fabrics are displayed in the Fabrics quick view of the Storage Environment dashboard. When you expand a fabric
branch to view its components, the list of components varies depending on the type of fabric as follows:
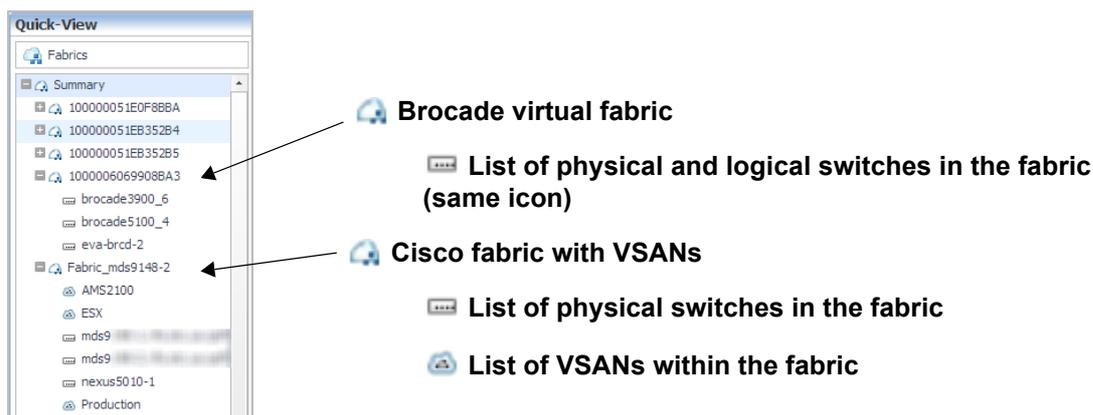
This walkthrough introduces the quick views for fabrics and their components.

To monitor fabrics, switches, and VSANs:

1   On the Storage Environment dashboard, ensure the **Monitoring** tab is selected.

2   Click the **Fabrics** tile to open the Fabrics quick view.

>   **TIP:** You can also open this quick view from the navigation panel. For more information, see
>   Introducing the Storage Explorer.

3   To identify the busiest fabrics in your environment, in the Fabrics list, click **Summary**.

     The Fabrics Summary (All Fabrics) panel opens. The Fabrics view identifies the top three fabrics with the
     highest average values for Data Rate, Link Error Rate, and Non-Link Error Rate, respectively. The FC
     Switches view identifies the top three switches in terms of the same metrics. The charts plot the metric
   values over the time period, while the tables show the average and current values for each component.
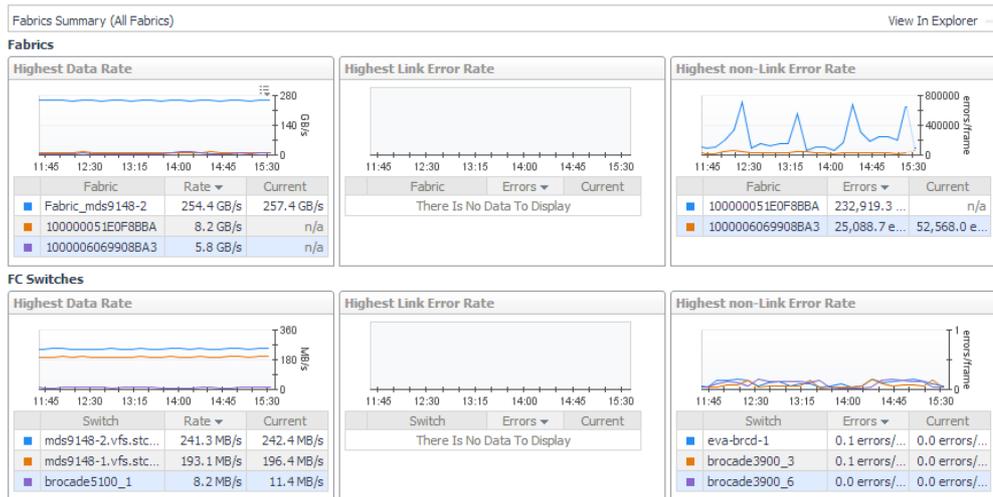
To investigate one of the top three fabrics or switches:

- To explore a top fabric, click its name in a table. See Exploring a Fabric.

- To explore a top switch, click its name in a table. See Exploring a Switch.

- To return to this quick view, in the breadcrumbs, click **Storage Environment**.

4   To monitor the performance of a fabric, in the Fabrics list, click a fabric name.

In the Fabric Summary (*Selected Fabric*), the Related Inventory view contains alarm summaries for the selected fabric as well as its switches, ISL ports, N ports, and VSANs (Cisco fabrics only). The Resource Utilization charts display the following metrics for ISL ports (left) and N ports (right) used by the fabric:

- **Avg Utilization Distribution**. For each type of port, displays aggregated values for Rcvd Utilization and Xmit Utilization grouped by percentage of usage. Most of your port utilization should be in the lower percentages. When there are ports performing at high utilization rates, you may want to investigate port performance further.

- **Data Rate**. For each type of port, plots aggregated values for Data Receive Rate and Data Send Rate over the time period and displays the Baseline.

- **Error Rate**. For each type of port, plots aggregated values for Link Error Rate and Non-Link Error Rate over the time period.
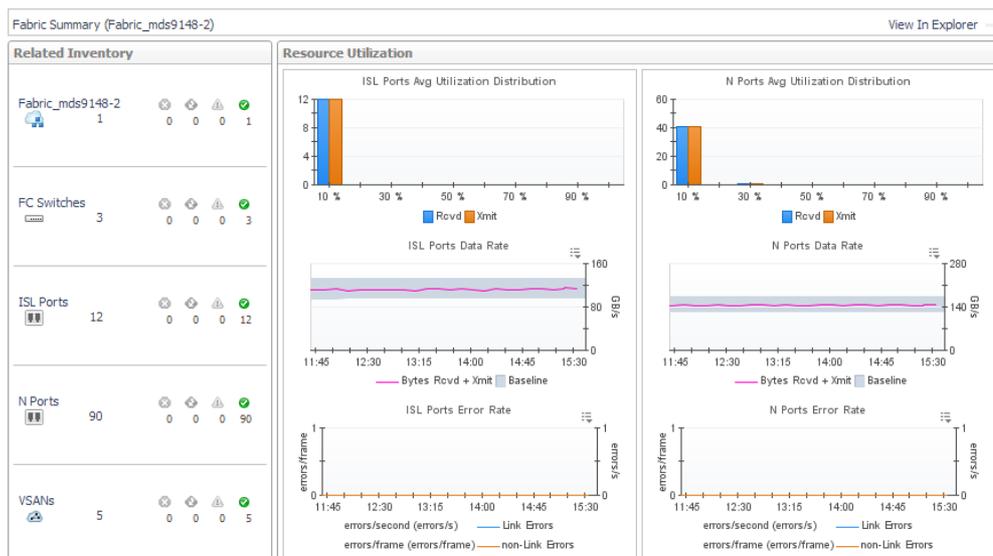

To continue investigating the selected fabric:

- To explore details about the fabric, its switches, and its ports, click **View in Explorer**. See Exploring a Fabric.

- To explore an FC switch in the selected fabric, in the Related Inventory view click **FC Switches** or an alarm icon, and select a switch. See Exploring a Switch.

- To investigate a port used in the selected fabric, in the Related Inventory view click either **ISL Ports** or **N Ports** or an alarm icon, and select a port. See Investigating an FC Switch Port.

- *Cisco fabrics only* —To investigate a VSAN used in the selected fabric, in the Related Inventory view click **VSANs** or an alarm icon, and select a VSAN. See Exploring a Cisco VSAN.

- To return to the quick view, in the breadcrumbs, click **Storage Environment**.

5   To monitor the performance of a switch (physical or logical), in the Fabrics list, expand a fabric and click a switch.

In the FC Switch Summary, the Related Inventory view contains alarm summaries for the selected switch, the fabric it belongs to, and its ISL ports and N ports. The charts display the following metrics for ISL ports and N ports used by the switch:

- **Ports Average Utilization Distribution**. For each type of port, displays aggregated values for Rcvd Utilization and Xmit Utilization grouped by percentage of usage. Most of your port utilization should be in the lower percentages. When there are ports on the switch performing at high utilization rates, you may want to investigate port performance further.

- **Rcv Rate**. For each type of port, plots aggregated values for Data Receive Rate over the time period and displays the Baseline.

- **Xmit Rate**. For each type of port, plots aggregated values for Data Send Rate over the time period and displays the Baseline.

- **Error Rate**. For each type of port, plots aggregated values for Link Error Rate and Non-Link Error Rate over the time period.
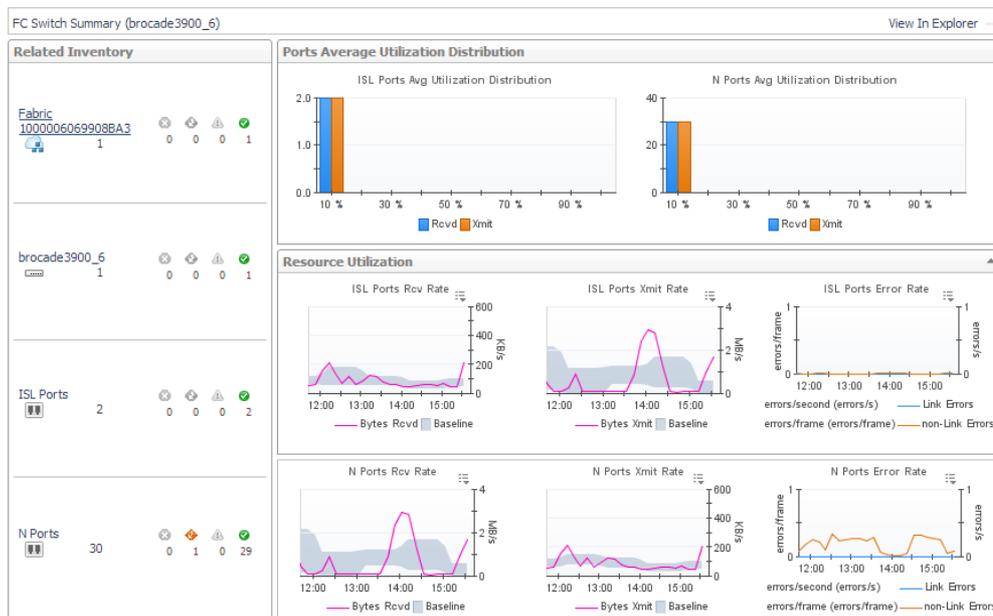

> ℹ️ **TIP:** To identify port performance that has changed, look for values that fall outside the grey Baseline ribbon.

To continue investigating the selected switch:

- To explore details about the switch and its ports, click **View in Explorer**. See Exploring a Switch.

- To investigate a port used by the selected switch, in the Related Inventory view click **ISL Ports** or **N Ports** or an alarm icon, and then select a port. See Investigating an FC Switch Port.

▪ To return to the quick view, in the breadcrumbs, click **Storage Environment**.

6 To monitor the performance of a Cisco VSAN, in the Fabrics list, expand a Cisco fabric and click a VSAN.

In the VSAN Summary, the Related Inventory view contains alarm summaries for the selected VSAN, the fabric it belongs to, and the ISL ports and N ports used by the VSAN. The Resource Utilization charts are the same as the charts displayed for a fabric, but the aggregated values include only the ports used by the VSAN.
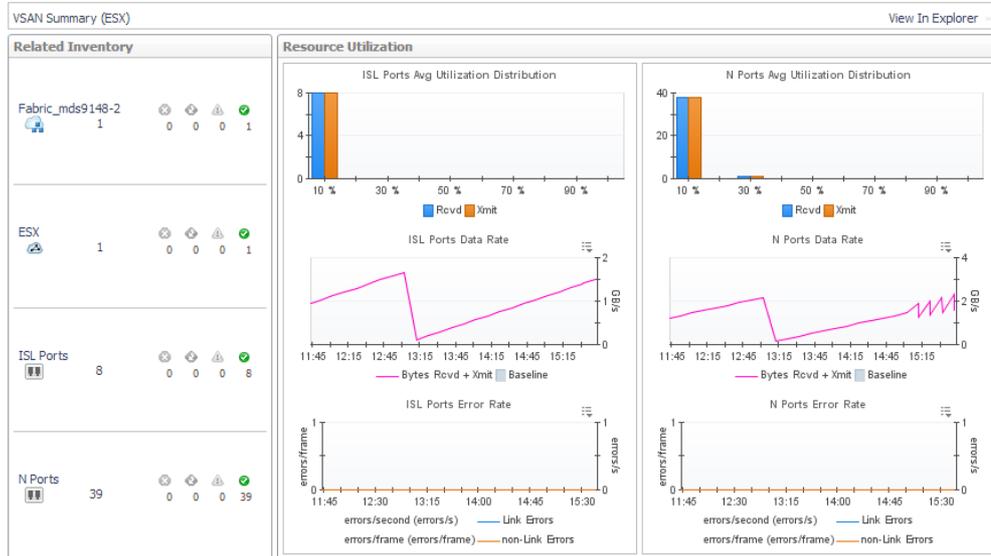
To continue investigating the selected VSAN:

▪ To explore details about the VSAN and its ports, click **View in Explorer**. See Exploring a Cisco VSAN.

▪ To investigate a port used by the selected VSAN, in the Related Inventory view click **ISL Ports** or **N Ports** or an alarm icon, and then select a port. See Investigating an FC Switch Port.

▪ To return to the quick view, in the breadcrumbs, click **Storage Environment**.

Monitoring Storage Arrays

When monitoring storage arrays, or when diagnosing alarms on storage arrays, you may need more detail on the array or its member nodes, controllers, ports, pools, LUNs, or disks. You may also want to determine if any of the child components have alarms that did not affect the array status. This walkthrough introduces the quick view for storage arrays.

To monitor storage arrays:

1 On the Storage Environment dashboard, ensure the **Monitoring** tab is selected.

2 Click the **Storage Arrays** tile to open the Storage Arrays quick view.

    i | **TIP:** You can also open this quick view from the navigation panel. For more information, see Introducing the Storage Explorer.

3 To identify the most problematic arrays in your environment, in the Storage Arrays list, click **Summary**.
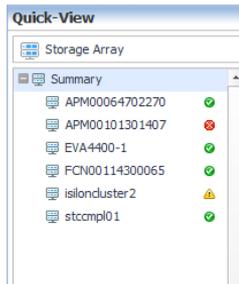
The Storage Array Summary summarizes the capacity and performance health of the arrays in the environment.

- Capacity

  - The table is organized by arrays whose pools have the most significant, near-term capacity issues.

  - The categories take into account the estimated time when pool capacity will be full, as well as the current available capacity and the over-provisioning state of the pool.

  - To investigate, click on the array name. See Monitoring Storage Capacity.

- Performance

  - The table is organized by arrays with the most LUNs having latency issues.

  - To investigate, click on the array name in the table to drill down to the Array Explorer. Click on the **LUNs** tab. See Investigating a LUN.

4   To monitor a storage array, in the Storage Array list, click a storage array name.

The content of the quick view varies depending on the selected storage array. For most storage arrays (excluding Dell EqualLogic and EMC Isilon), the quick view contains the following embedded views:

- **Related Inventory**. Contains alarm summaries for the selected storage array and its controllers, FC ports, IP ports, pools, LUNs, and disks.

- **Storage Capacity Summary**. Displays current values for Total Advertised LUNs Size and Capacity Provisioned to LUNs.

- **Controller Performance**. Plots % Busy values by controller over the time period and displays threshold lines (defined in registry variable *StSAN.Controller.PctBusyThreshold*).

- **Pools with Severe or High Pressure on Available Usable Capacity** (or Raw Capacity)

  - Displays the pools that have the most significant, near-term capacity issues.

  - Shows the available usable capacity or available raw capacity in the table, depending on the data provided from the device vendor, and the % available.

  - Shows the estimated time when the pool capacity will be full

  - Over commitment is not shown when raw capacity numbers are displayed.

□ The cylinders are colored to show the % of available capacity in the pool.

▪ **LUNs/Disks States**. Plots the percentage of disks and LUNs in the storage array in problem states. Problem states are reported by the vendor. Resolving these issues may improve LUN performance.
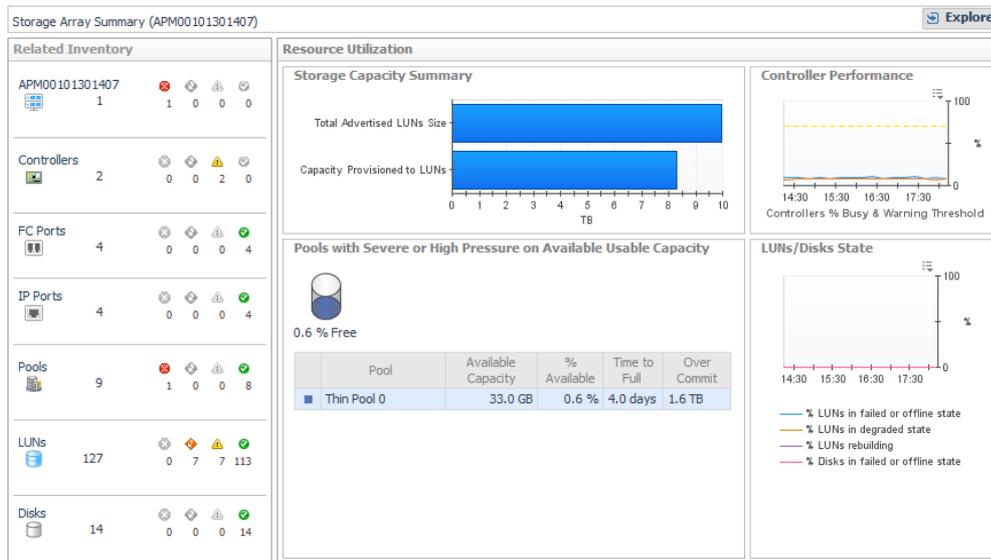
For more storage array quick views, see the Summary tab description under Dell EqualLogic Storage Array and EMC VPLEX Storage Array.

5   To continue investigating the selected storage array:

▪ To explore details about the storage array and its child components, click **View in Explorer**. See Exploring a Storage Array.

▪ To investigate a child component, in the Related Inventory view click a component type or a status icon, and then select a component. A component dashboard opens. For help with the dashboard, see one of the following topics:

- Investigating a Controller

- Investigating an EqualLogic Member

- Investigating an Isilon Node

- Investigating an Array/Filer Port

- Investigating a Pool

- Investigating a LUN

- Investigating a Physical Disk

▪ To return to this quick view, in the breadcrumbs, click **Storage Environment**.

Monitoring Filers

When monitoring filers, or when diagnosing alarms on filers, you may need more detail on a filer and its controllers, ports, NASVolumes, LUNs, aggregates, or disks. You may also want to determine if any child components display alarms. This walkthrough introduces the quick views for filers.

To monitor filers:

1   On the Storage Environment dashboard, ensure the **Monitoring** tab is selected.

2   Click the **Filers** tile to open the Filers quick view.

TIP: You can also open this quick view from the navigation panel. For more information, see Introducing the Storage Explorer.

3   To identify the busiest filers in your environment, in the Filers list, click **Summary**.
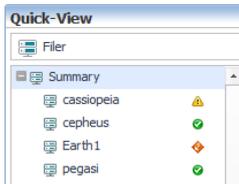
The Filer Summary view identifies the top three filers in two categories:

- **Filers with Lowest % of Free Disk/Spares Capacity (raw)**. Displays cylinders showing the amount of used Free Disk/Spares Capacity (Raw). Below each cylinder, you can see total and free capacity.

- **Filers with Lowest % of Available Aggr Capacity (usable)**. Displays cylinders showing the amount of used Aggr Capacity (Usable) Free. Below each cylinder, you can see total and free capacity.
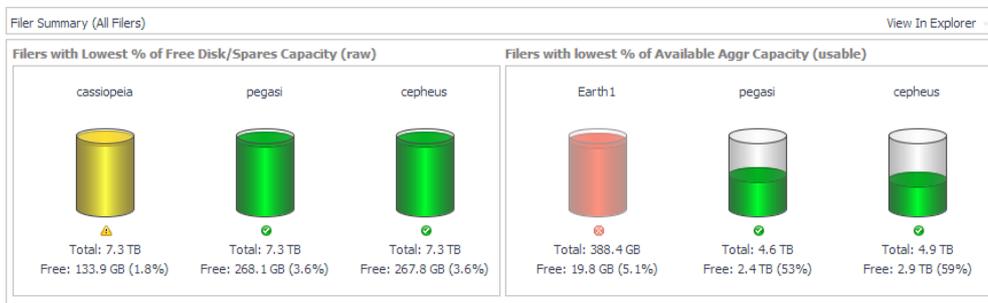
If you find that cylinder colors do not reflect the acceptable thresholds in your environment, you can ask your Foglight for Storage Management Administrator to edit the threshold values in the following registry variables:

- **Disk capacity**: *StSAN.FilerDisks.PctUnallocatedCapacityThreshold.[Fatal|Critical|Warning]*

- **Aggregate capacity:**
  StSAN.FilerAggregates.PctUnallocatedCapacityThreshold.[Fatal|Critical|Warning]

NOTE: Registry variables are global variables that are often referenced by rules. Before editing a registry variable, ensure that the edit will not cause unintended changes to how the affected rules trigger alarms. For more information, search for "Registry Variable" in the online help.

4   In the Filer list, click a filer name.

The Related Inventory view contains alarm summaries for the selected filer as well as its controllers, ports, NASVolumes, LUNs, aggregates, or disks. The Resource Utilization charts show capacity and performance metrics for the filer:

- **Storage Capacity Summary**. The cylinders show the amount of capacity consumed in the filer, expressed using current values for the following pairs of metrics:

  - Disk Capacity (Raw) and Free Disk/Spares Capacity (Raw)
  - Aggr Capacity (Raw) Total and Aggr Capacity (Raw) Free
  - Aggr Capacity (Usable) Total and Aggr Capacity (Usable) Free

  The bar chart displays current values for Advertised LUN Size, Advertised NASVolumes Size, Aggr Capacity (Usable) Total, and Aggr Capacity (Usable) Free.

- **NASVolume Performance**. Plots the percentage of NASVolumes in the filer in problem states. Problem states are reported by the vendor. Resolving issues may improve volume performance.

▪ **LUN Performance**. Plots the percentage of LUNs in the filer in problem states. Problem states are reported by the vendor. Resolving issues may improve LUN performance.

5   To continue investigating the selected filer:

▪ To explore details about the filer and its child components, click **View in Explorer**. See Exploring a Filer.

▪ To investigate a child component, in the Related Inventory view click a component type or an alarm icon, and then select a component. A component dashboard opens. For help with the dashboard, see one of the following topics:

- Investigating a Controller

- Investigating an Array/Filer Port

- Investigating a NASVolume

- Investigating a LUN

- Investigating an Aggregate

- Investigating a Physical Disk

▪ To return to this quick view, in the breadcrumbs, click **Storage Environment**.

Asking Questions About the Monitored Storage Environment

Another way to find out information about your storage environment is to ask questions. The *Insights* tab contains the *Analytics* view to show frequently-asked questions about storage environments. Answers are displayed in the form of tables and graphs. You can select questions that apply to all storage resources or to a specific type of storage resource.

To use the Insights > Analytics view:

1   On the Storage Environment dashboard, click the **Insights** tab, and then click **Analytics**.

2   In the Categories pane, click a category to display the questions for that category in the Questions pane.

> **i** | **TIP:** If the list of questions is long and you want to narrow it down, search for a particular text string using the **Search Questions** box.

3   In the Questions pane, click a question to display the answer in the Answer pane.
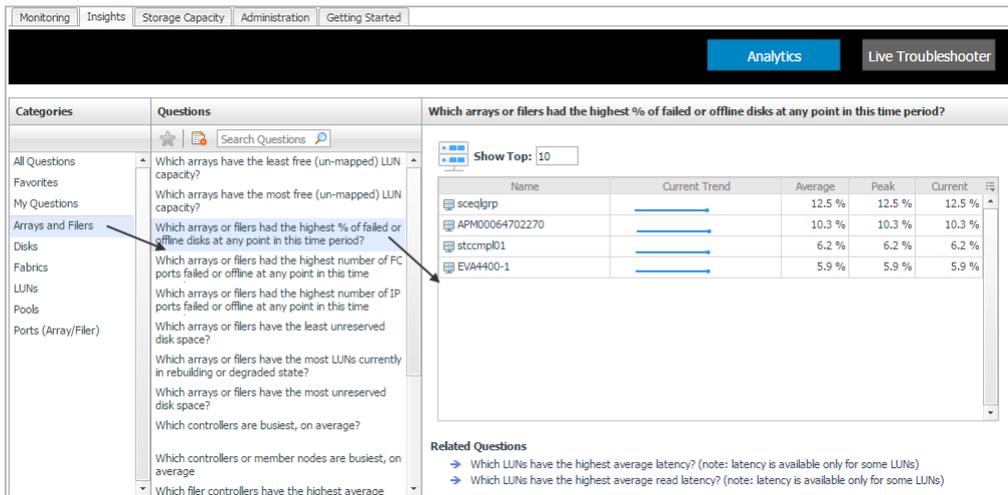
4 In the Answer pane, you can change the number of results displayed by changing the value of the Show Top box.

5 To investigate a component or its parent device, click a name in the Name or Parent column.

Assessing Connectivity and I/O Performance

You can also identify connectivity and port performance problems that occur during I/O requests by assessing storage from the perspective of the virtualization environment. The VMware and Hyper-V Explorers offer an end-to-end look at all the entities that make up your virtual infrastructure, including clusters, hosts, virtualization storage, and virtual machines.

> **i** | **NOTE:** This workflow assumes that the following requirement is satisfied:
>
>   ▪ VMware or Hyper-V Performance agents are defined for the target environment, and the agents are configured to collect storage data. For more information, see Step 2 in Collecting Storage Data for Virtualized Devices and Servers.

This section covers the following topics:

- Introducing the Virtualization Dashboards

- Summary of Icons Used in Topology Diagrams

- Exploring Connectivity with SAN Topology Diagrams

- Exploring I/O Performance with SAN Data Paths

Introducing the Virtualization Dashboards

This workflow introduces you to the version of the Virtualization dashboards available in Foglight for Storage Management. For detailed information, see the *VMware Monitoring in Foglight for Storage Management User and Reference Guide* or *Hyper-V Monitoring in Foglight for Storage Management User and Reference Guide*.

Table 15. List of dashboards that display virtualization storage environment-to-SAN relationships when data collection is enabled on VMware or Hyper-V Performance agents

Dashboard	SAN Topology Tab	SAN Data Paths Tab
ESX Host/Hyper-V Server	Yes	Yes
Virtual Machine	Yes	Yes
Cluster	Yes	—
Datastore, CSV, logical disk	Yes	—
LUN	Yes	Yes
NASVolume	Yes	—

The following workflow walks you through opening a virtualization dashboard and selecting an entity to explore.

To use the virtualization dashboard and topology diagrams:

1   On the navigation panel, under Dashboards, click either **VMware > VMware Explorer** or **Hyper-V > Hyper-V Explorer.**

> **i** | **TIP:** If you do not see the menu, ask your Foglight for Storage Management Administrator to add the role *VMware Administrator* or *Hyper-V Administrator* to your user account.

The Explorer opens an Infrastructure menu below the Dashboards menu on the navigation panel.

2   Under **Infrastructure**, on the **Topology** tab, select the desired entity.

The dashboard opens.

> **i** | **NOTE:** The topology will display clusters, virtualization servers, and virtual machines. For VMware, it will display Virtual Centers and Datacenters.

- From the Summary tab, you can monitor and investigate entities in your virtual infrastructure using an approach similar to the Storage Environment dashboard.

- When you click the Storage tab, you see a list of all logical storage used by the entity and the associated storage capacity. Click a storage entity name to open the dashboard containing details about the entity.
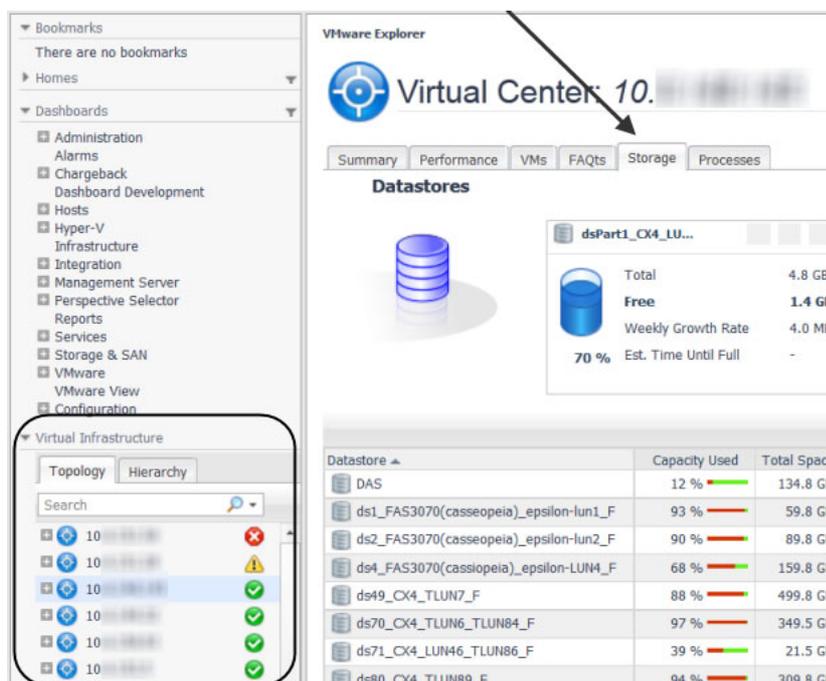
> **TIP:** When the list of entities is long—which is often the case for virtual machines—you can find an entity by typing its full or partial name in the Topology tab's Search box.

When you select a cluster, the dashboard will include SAN Topology tabs. Host/server and virtual machine dashboards will include SAN Data Paths views in addition to SAN Topology that you can explore.

- **Click the SAN Topology** tab. For instructions about this view, see Exploring Connectivity with SAN Topology Diagrams.
- **Click the SAN Data Path** tab. For instructions about this view, see Exploring I/O Performance with SAN Data Paths.

Summary of Icons Used in Topology Diagrams

In topology diagrams, the icons represent entities in your monitored virtual infrastructure and storage infrastructure, as described in the following table. Each icon incorporates a small status icon to show the status of the entity.

Table 16. Icons used in topology diagrams.

Icon	Represents	Description
	Physical Host	A physical server in your network.
	ESX Host	A physical server hosting the hypervisor-based architecture and virtual machines controlling and managing resources for the virtual machines.
	Hyper-V Server	
	Virtual Machine VMware	A virtual machine running on a host or server.
	Hyper-V	
	Datastore	A datastore or CSV (Cluster Shared Volume) or logical disk is a logical storage structure used to provide virtual machine disks and files.
	Logical Disk	
	CSV	
	Disk Extent	A disk extent is all or part of a host disk that can provide the physical storage for a datastore, CSV or logical disk. The disk extent can be on a local DAS device, or it can be mapped to a LUN on a storage array or filer in the SAN.
	Cloud	Hides port-level complexity in a topology diagram. Click the icon to view ports and their connected devices in a Detail window. **NOTE:** The SAN Data Paths tab does not use the cloud icon. All ports and their devices are shown in the diagram.

Table 16. Icons used in topology diagrams.

Icon	Represents	Description
	FC Port	FC ports connect to other FC ports on switches, physical hosts, storage arrays, or filers using fibre-channel network technology in the SAN.
	IP Port	IP ports provide access to the IP network for storage devices using iSCSI or other protocols.
	Controller	A controller manages the ports used by a storage array or filer.
	LUN	A LUN (logical unit number) represents a logical SAN block storage device on an array or filer that can be exposed for mapping to a server.
	NASVolume	A NASVolume is a volume whose physical storage is on a filer or unified storage supplier. It can be mounted by an ESX host to provide the physical storage for a datastore using NFS.
	Member or Node	A storage server that works together with other members or nodes in a clustered storage architecture. The array cluster distributes the workloads among the members of the cluster.
	Logical Interface	In Netapp cluster mode, users access storage by SVMs. Connectivity to SVMs is provided through logical interfaces (LIFs). A LIF has an IP address or a World Wide Port Name, used by a client or host to connect to an SVM.

Exploring Connectivity with SAN Topology Diagrams

SAN Topology diagrams map the connections through the virtual environment (VMs-to-virtualization storage-to-extents) to the resources in the SAN (LUNs and NASVolumes). Topology diagrams hide port-level details to focus on connectivity. Using this view, you can see which resources have an alarm status along each connection path, and begin to form hypotheses about whether or not the SAN environment is contributing to performance issues in the virtual environment. You can then drill down on resources to test those hypotheses.

In a topology diagram, you can view individual port connections by clicking one or more cloud icons. Details are shown in a separate window.

> **i** | **TIP:** If your primary goal is to assess the performance of the ports that are used by the datastores and disk extents connecting to the SAN, use the SAN Data Paths tab instead (when available). For more information, see Exploring I/O Performance with SAN Data Paths.

The SAN Topology view displays as a graph for a VM, Datastore or CSV, and for a storage LUN or NASVolume.

The SAN Topology view for a Cluster or server or host will offer the following choices for viewing the topology:

- Show Datastore or CSV resources used by VMs as graph
- Show RDM or pass-through disk resources used by VMs as graph
- Show storage resources used by VMs as table
- Show all storage resources as table

The option to show all storage resources as a table will include Datastores or CSVs that are not used by VMs.

The following workflow explains how you can verify connectivity and the status of entities and storage devices in your infrastructure using a topology diagram. This procedure assumes that you navigated to a topology view from a Virtualization Explorer dashboard (see Introducing the Virtualization Dashboards) or from a Storage Explorer component dashboard (see Investigating a LUN or Investigating a NASVolume).

To use a topology diagram graph:

1   Click on a Datastore or CSV icon to see the VMs that use this storage. Click on a cloud icon to see the extents that map to the LUN.

> ℹ | **NOTE:** When viewing the graph for a Cluster, the VMs and disk extents are not displayed on the main graph. When viewing the graph for a server or host, if it supports large numbers of VMs, as in a VDI environment, the VMs will not display on the main graph.

The following image shows virtual machines connected to separate datastores. The disk extents are identified and linked through the network to LUNs. For descriptions of icons, see Summary of Icons Used in Topology Diagrams.
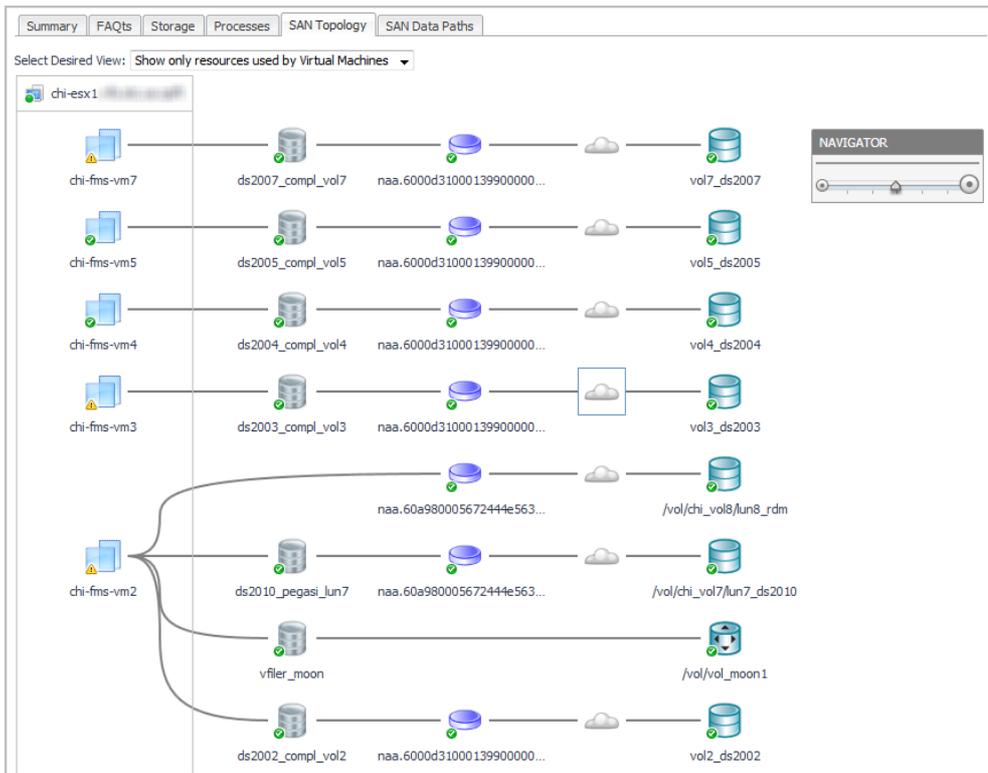

2   When a topology diagram has a very large number of elements to be displayed, the graphical representation may be changed to a table for clarity. If the graph is too large to display in the viewing area, you can use the browser's scroll bars and the Navigator to view the hidden areas. The Navigator enables you to scale the topology diagram and, in large diagrams, drag the viewing area to a different part of the diagram.

3   Click a Datastore or CSV icon to see the VMs that use this storage.
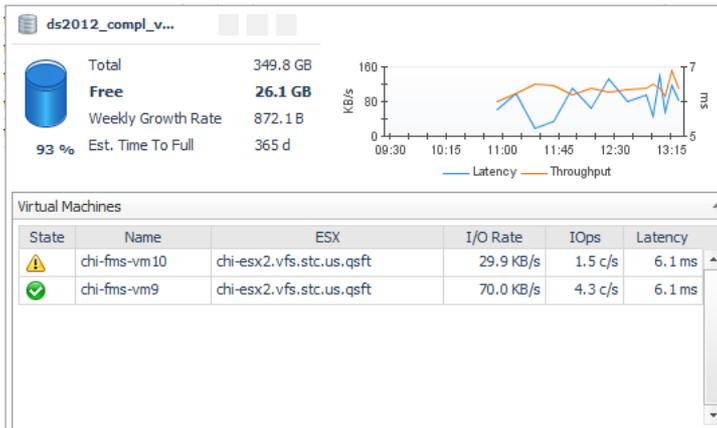
4   Click any icon to review key details and metrics about the entity.
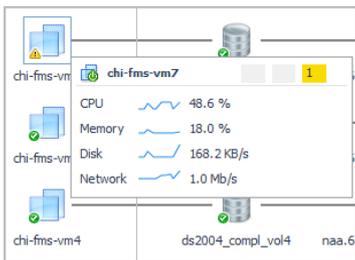
5   Click a **Cloud** ☁ icon to display the ports and SAN paths from the logical storage to the LUN, through the host or server.
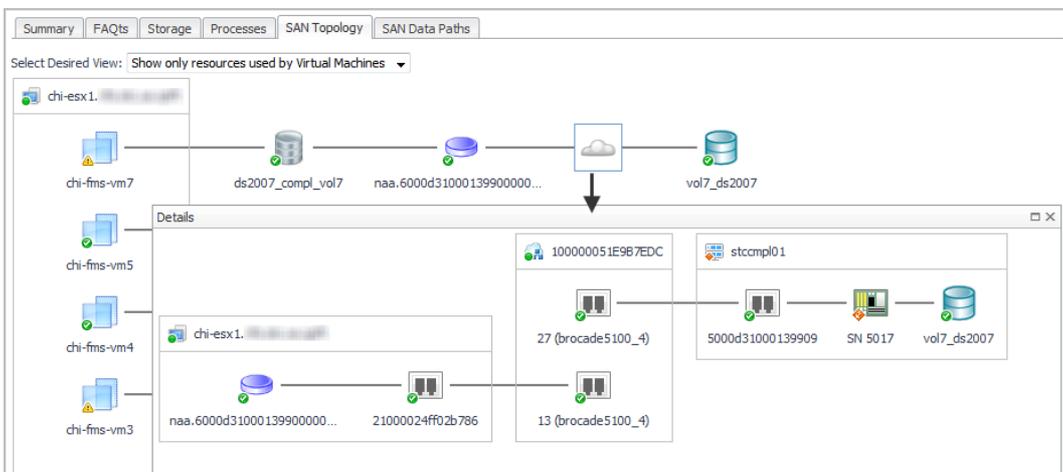
In this example, you can see that the LUN's controller has a Critical status.

6   To investigate an entity, click its icon. For example:

    a   Click the controller 🎛 icon.

    b   To view the alarm message, click the alarm count (opens an Alarm Summary window) or the controller name (opens the Controller dashboard).
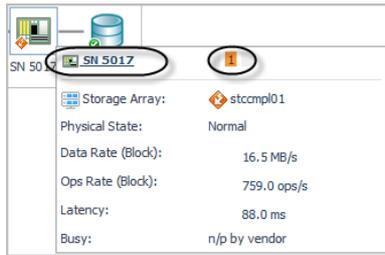
c   The Alarm Summary reports the cause.

7   In some topology diagrams, you may see an inferred host (indicated with an orange line). On these diagrams, if an inferred-host-to-port assignment is incorrect, you can click the host port icon and click the appropriate action to correct it.
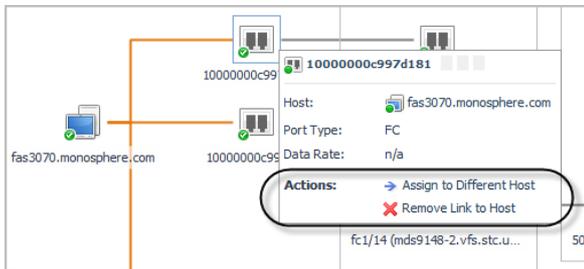
To use a topology diagram table:

1   Click on a VM cell to display the VMs that use this Datastore or CSV, or RDM. Click on a cloud icon to display the ports and SAN paths from the storage to the LUN, through the hosts or servers.

> **NOTE:** The table view provides the same information as the graphical view.

Exploring I/O Performance with SAN Data Paths

The SAN Data Paths tab focuses on input/output performance of the ports used in the data paths connecting the virtual environment to the SAN. This view combines an I/O Data Paths table with a topology diagram that includes port details and I/O performance metrics. The table displays the worst-performing path segment of the possible data paths between each disk extent and the LUN during the time period, helping you to identify bottlenecks resulting in high latency. The diagram enables you see the entities that are capable of doing I/O through each path segment, corresponding to the table rows.

Because the metric values in the SAN Data Paths tab represent the average values over the time period, consider selecting a shorter time range (one hour or less) to help investigate performance spikes. For example, if a customer is complaining about latency issues in the last 15 minutes, you may want to set the dashboard time range to the last 15-30 minutes to focus on the problem period.

> **TIP:** If your primary goal is to discover which SAN resources are used by entities in your virtual environment, use the SAN Topology tab instead. For more information, see Exploring Connectivity with SAN Topology Diagrams.

This workflow walks you through using the SAN Data Paths tab from the VMware Explorer's ESX Host dashboard. The content of the SAN Data Paths tab may be slightly different on the Virtual Machine, Datastore, and LUN dashboards, but the flow is the same. The workflow for Hyper-V servers, VMs, and CSVs is similar, but uses the Hyper-V terminology. This workflow continues from Introducing the Virtualization Dashboards.

To review data paths:

1. On the SAN Data Paths tab, review the In Use I/O Paths table to see the worst-performing path segments in terms of Latency.

   The color of the bars (in the table and in the diagram) highlights data values that fall within various thresholds. Metrics without thresholds are displayed in dark blue.

   The columns display the following details and metrics. On the Virtual Machine, Datastore, and LUN dashboards, the details and metrics may be slightly different.

   - **Datastore/Disk Extent**. List of datastores and the disks that they use, ordered so that the datastores with high-latency disk extents appear at the top. Datastores configured from a NASVolume show only the associated volume; no other data is available. If an *RDM* or *Other* node is displayed, the disk extents under this node are RDMs providing storage directly to the virtual machine.

   - **Latency**. Average latency per operation.

     > **NOTE:** When physical hosts are inferred, latency values are unavailable because the disk extents that map to the selected LUN are unknown. For more information, see Inferring Physical-Host-to-Storage Relationships.

   - **Data Rate**. Average data rate for I/O from the ESX or VM to the LUN.

   - **ESX FC Ports --> SAN Util**. Displays the busiest link (read or write utilization) in the possible paths between the ESX and the FC switches. Click the cell to display all the port links. Review the topology diagram to see the ports and link utilization. Data is not available for IP ports.

   - **SAN --> A/F Ports Util**. Displays the busiest link (read or write utilization) in the possible paths between the FC switches and the array/filer ports. Click the cell to display all the port links. Review the topology diagram to see the ports and link utilization. Data is not available for IP ports.

   - **A/F Ctrl Busy**. Displays the CPU % Busy metric for the busiest controller in the data path for a storage array or filer. % Busy values are not available on some devices.

   - **LUN / NASVolume / Dir**. Displays the LUN that is mapped to the extent, or displays the NASVolume (filers) or directory (Isilon arrays) providing the storage for a datastore.

- **% Competing I/O at LUN**. Displays the percentage of I/O being experienced by this LUN for all VMs accessing the Datastore, not just those in this ESX. Click the cell to display the top five VMs doing I/O to this LUN.

- **LUN State**. Reports on the state of the LUN as follows:

Table 17. LUN states

⚠️	Indicates that the LUN is reporting activity that gives an indication of performance problems, it is currently degraded or rebuilding, or the % Busy or Latency metrics are over their thresholds for the time period. Dwell on the cell for details.
📝	Indicates that the vendor does not provide % Busy or Latency metrics.
✅	Indicates that either the % Busy metric or Latency metric is within normal range during the time period, and the LUN is not reporting that it is currently degraded or rebuilding. Dwell on the cell for details.

- **Latency (ms).** Average latency per operation to the LUN during the time period.

2 In the diagram, ensure that Select Desired View is set to **Show full data paths**.

The diagram shows the data paths between datastores and the LUNs providing the physical storage within an ESX host. The bars shown below the icons summarize average latency for hosts (if available), link utilization for FC ports, and percentage busy for controllers. For descriptions of icons, see Summary of Icons Used in Topology Diagrams.

Latency   Link utilization   Percentage busy

This diagram highlights how ports are often shared by multiple disk extents. You may be able to trace the cause of a poorly-performing disk extent to poor link utilization values or to some resource issue further down the data path in the SAN. Or if all SAN ports and resources are in a Normal status, you may be able to rule out a storage issue.

3 Review the data paths for the worst performing entities to identify bottlenecks that may be contributing to the high latency values.

4 To see more of the diagram, use the Navigator to shrink the diagram or move the viewing area. For more information, see Exploring Connectivity with SAN Topology Diagrams.

> **i** | **TIP:** You can also close the I/O Paths table using the arrow on the far right of the table title bar.

5 To investigate an entity, click its icon or name. Use the breadcrumbs to return to this view.

6   If you find that the colors used in some metric bars do not reflect acceptable thresholds in your environment, you can ask your Foglight for Storage Management Administrator to edit the threshold values in the following registry variables:

- **Latency**: *VMW:diskTotalLatency.[warning|critical|fatal]*

- **Latency:** *HPV:diskTotalLatency.[Warning, Critical, Fatal]*

- **Port utilization**: *StSAN.FCSwitchPort.Utilization.[Warning|Critical|Fatal]*

- **A/F Ctrl Busy**: *StSAN.Controller.PctBusyThreshold.[Warning|Critical]*

> **NOTE:** Registry variables are global variables that are often referenced by rules. Before editing a registry variable, ensure that the edit will not cause unintended changes to how the affected rules trigger alarms. For more information, search for "Registry Variable" in the online help.

Monitoring Storage Capacity

Foglight for Storage Management closely monitors the capacity being used by the pools in your array or filer. The historical growth of pool capacity usage is analyzed daily to estimate how much time is remaining until the pool becomes full. This capability is critically important for pools that are over-committed with thin-provisioned LUNs and/or NASVolumes.

This section discusses the rules and alarms, views, charts, reports, and configurable values you can use to monitor your pool capacity.

For details, see the following topics:

- Capacity Trending
- Evaluating Pool Capacity
- Environment Summary/Monitoring/Summary
- Capacity Reports
- Low Capacity Rule
- Storage Capacity tab

Capacity Trending

Foglight for Storage Management performs a linear regression analysis nightly on the historical values of consumed pool capacity.

The Time Until Full (per available history) will use all available history, up to the last 180 days, to project when the pool will become full. The minimum number of days required to compute this trend is defined by the registry variable *StSAN_minDaysForLongHistTrend*. The default is 30 days.

The Time Until Full (per limited history), will use only recent history, up to the last 30 days, to project when the pool will become full. The minimum number of days required to compute this trend is defined by the registry variable S*tSAN_minDaysForShortHistTrend*. The default is 20 days. Examining this value is useful primarily when there has been a significant recent change in the pool usage that is expected to continue.

The Time Until Full value is displayed with the following granularity:

- In days, for 0-2 months
- In weeks, for 2-6 months
- In months, for 6-12 months
- As "> 1 year", for anything beyond 365 days
- As "> 1 year" when usage is decreasing or not changing, not increasing.

- As "n/a" when there is insufficient history

The Time Until Full (available history) value is displayed on most screens that show pool date. The Capacity tab of a Pool Explorer will display a chart of the capacity and the trends.

Evaluating Pool Capacity

Pool capacity is evaluated every few hours (after a new topology collection) to determine if a low pool capacity alarm should be generated, and to summarize the number of pools experiencing capacity pressure on the Environment Summary/Monitoring/Summary for Arrays and Filers.

The following factors are examined to determine if a pool is experiencing capacity pressure.

- The over-committed state of the pool
- The absolute capacity available and the % of capacity available
- The estimated Time Until Full

Environment Summary/Monitoring/Summary

This view will provide you with a quick summary of the arrays in your environment, ordered by low score at the top. The score reflects the percent of pools in your environment with capacity issues.
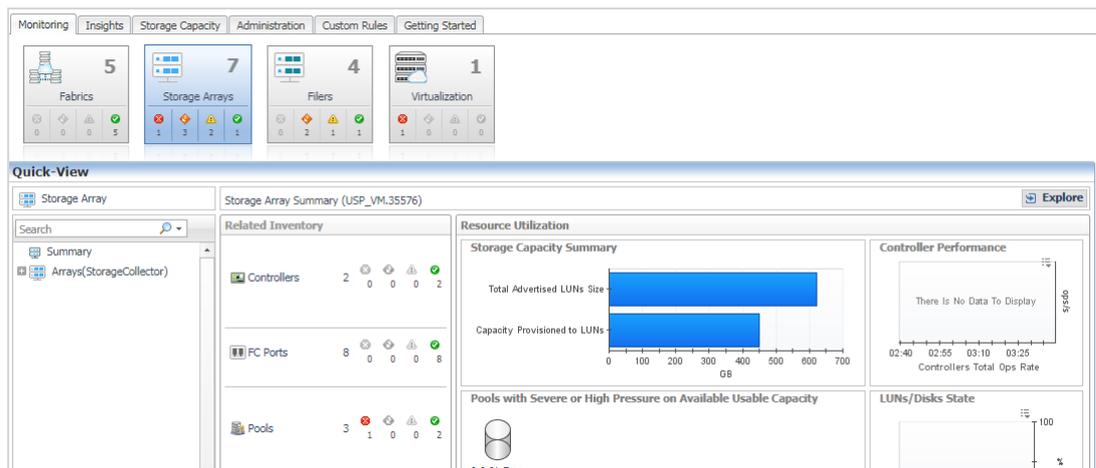
Clicking on the array name will display a view that identifies the pools with Severe or High capacity issues. A low pool capacity alarm will have been generated for every pool that is not OK, if the low pool capacity rule is enabled.
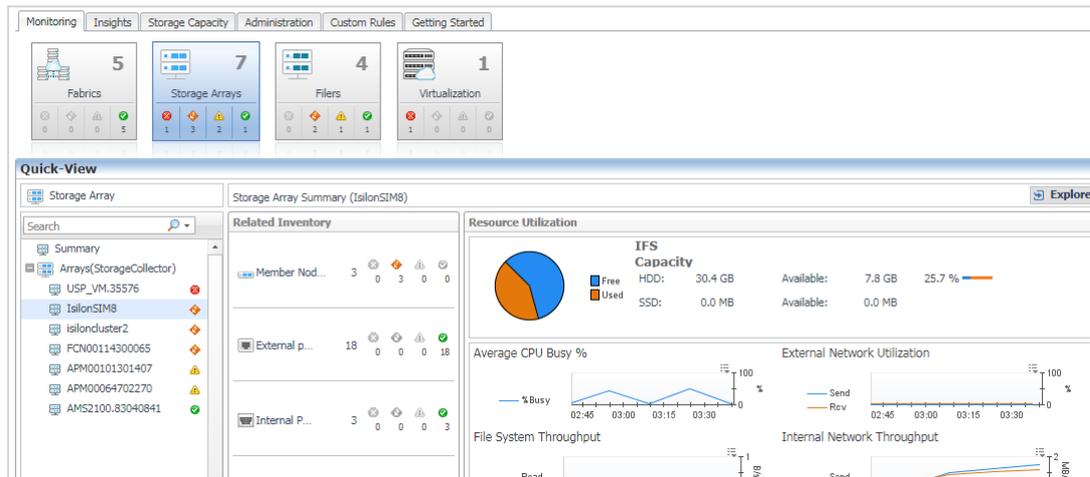
Capacity Reports

The SanStorage Pools Capacity Summary Report summarizes the total and available capacity, and estimated time until full, for the pools or aggregates in the selected Storage devices. The report can be optionally limited to the pools or aggregates with thin-provisioned entities.

Low Capacity Rule

The rule StSAN E Pool Low Available Capacity with Email will be evaluated after every collection that provides new capacity information. A fatal alarm will be generated for every pool experiencing severe capacity pressure. A critical alarm will be generated for every pool experiencing high capacity pressure. A warning alarm will be generated for every pool included under the monitor count. No email will be generated for warning alarms.

Registry Variables

The following registry variables are used in the pool capacity evaluations for alarm generation and for determining which pools are experiencing capacity pressure.

These variables are used in pool capacity evaluation to compare to the estimated Time Until Full. For over-committed pools, they will generate alarms as Fatal/Critical/Warning. For pools that are not over-committed, they will generate alarms as Critical or Warning, based on the available capacity in the pool.

- StSAN.Pool.TimeToFull.VerySoon - default 2 weeks

- StSAN.Pool.TimeToFull.Soon - default 4 weeks

- StSAN.Pool.TimeToFull.Warn - default 12 weeks

There variables are used to examine pool capacity when no estimated Time Until Full value is available, and when the Time to Full is very long. Critical or Warning alarms will be generated for pools that are not over-committed. Fatal and Critical alarms will be generated if the pool is over-committed.

- StSAN.Pool.AvailableCapacityThreshold.Critical - default 100 GB

- StSAN.Pool.AvailableCapacityThreshold.Warning - default 200 GB

- StSAN.Pool.PctAvailableCapacityThreshold.Critical - default 5%

- StSAN.Pool.PctAvailableCapacityThreshold.Warning - default 10%

The value of these registry variables can be easily modified to meet the needs of your environment.

Storage Capacity tab

The Storage Capacity tab includes charts and tables for monitoring the capacity being used by the all devices, pools, LUNs, NASVolumes, or aggregates. Select what you want to monitor by clicking one of the following button at the top of the view: **All, Pools, LUNs, Volumes,** or **Aggregates**.

The middle part of the view includes the Storage Capacity chart, which shows the pools with the scatter chart that uses Free as Y axis and Capacity Available Percent as X axis.

The lower part of the view includes the Storage Capacity table, which displays the following information for the selected option (All, Pools, LUNs, Volumes, or Aggregates).

Table 18. Storage Capacity table

Screen Element	Description
Name	Device name.
	Click the name to open the device Summary tab.
Type	Device type.
Array/Filer	Array or filer name.
Time to Full	Time remaining until the maximum capacity is reached.
Health Score	Health score. For details about how health scores are calculated, see Pool and Volumes health scores.
Capacity Used (% Available)	Capacity currently used.
Free	Capacity currently available (free).
Total	Total device capacity.

Pool and Volumes health scores

Health scores are base on two criteria:

- How much free space exists.
- How much time is left until that space runs out.

Pool health scores

The code is in a derived metric, so that the heath scores are recalculated on the fly, whenever new data for a pool is submitted. The code works as follows:

Starting score: 75%

If long term (preferred) or short term predictive data is available, the starting score is reset:

< 14 days to full: set to 10%

< 28 days to full: set to 35%

< 84 days to full: set to 50%

> 300 days to full: set to 100%

> 200 days to full: set to 85%

> 100 days to full: set to 70%

From the starting score, the code adjusts the calculations based on the percent of free space available:

< 10%: score adjusted -30%

< 20%: score adjusted -20%

< 30%: score adjusted -10%

> 90%: score adjusted +30%

> 80%: score adjusted +20%

> 70%: score adjusted +10%

Any computed values over 100 are changed to 100%.

Any computed values < 0 are changed to 0%.

Volume health scores

Trending data for volumes is not available yet. Therefore, the health score is currently based solely on the currently available capacity.

> **i** | **NOTE:** Once the trending data becomes available for volumes, the same rules for calculating pool health score would apply to volumes as well.

The code works as follows:

Starting score: 75%

From the starting score, the code adjusts the calculations based on the percent of free space available:

< 10%: score adjusted -30%

< 20%: score adjusted -20%

< 30%: score adjusted -10%

> 90%: score adjusted +30%

> 80%: score adjusted +20%

> 70%: score adjusted +10%

Any computed values over 100 are changed to 100%.

Any computed values < 0 are changed to 0%.

Creating Storage Reports

In the Storage Environment dashboard, you can create reports to share with colleagues. You can also copy and edit existing reports. If the Reports tab is not displayed, your Foglight for Storage Management Administrator may need to modify your user account to include the *General Access* role.

> **i** | **TIP:** You can also use the Foglight for Storage Management Reports dashboard available from the Reports link at the top of all dashboards. For more information about this dashboard, see the *Foglight User Guide*.

To create a report:

1   On the Storage Environment dashboard, click the **Insights** tab, and then click **Reports**.

The Create a Report wizard opens. Use the **Next** and **Back** buttons to navigate between pages.

Follow the steps in the wizard to select a report template and specify report parameters.
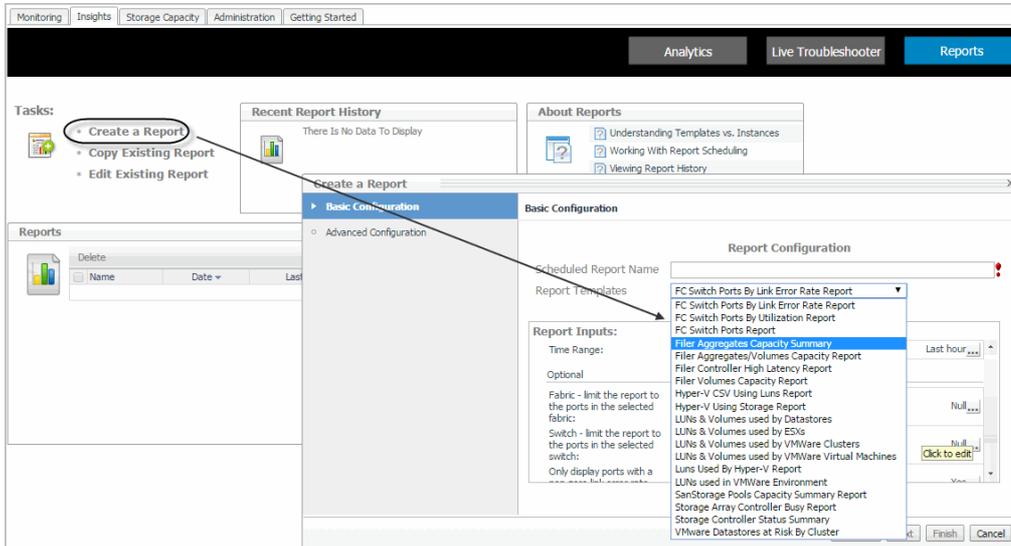
2   Click **Finish** to generate the report.

Investigating Storage Devices

To find out more about the performance of a storage device and its components, you use the Storage Explorer dashboards.

This section covers the following topics:

- Introducing the Storage Explorer
- Exploring a Fabric
- Exploring a Switch
- Exploring a Cisco VSAN
- Exploring a Filer
- Exploring a Storage Array

Introducing the Storage Explorer

The Storage Explorer enables you to quickly find and examine any storage device in your storage environment. The Storage Explorer has a Topology tree—displayed in the navigation panel below the list of Dashboards—that contains branches for Fabrics, Filers, and Storage Arrays. The fabrics in the Fabrics branch can be expanded to show FC switches and VSANs. When you select a device from the tree, the Storage Explorer opens a dashboard displaying details about that device.

This walkthrough describes how to open the Storage Explorer and select a storage device. If you select a top-level device type node, such as Fabrics, the Storage Environment quick view is displayed. For more information about the quick view, see Summary and Resource Information for each Collected Target:.

To use the Storage Explorer:

1   On the navigation panel, under Dashboards, click **Storage & SAN** > **Storage Explorer**.

    The Topology tree opens below the Dashboards area, containing a list of all monitored storage devices and their status.
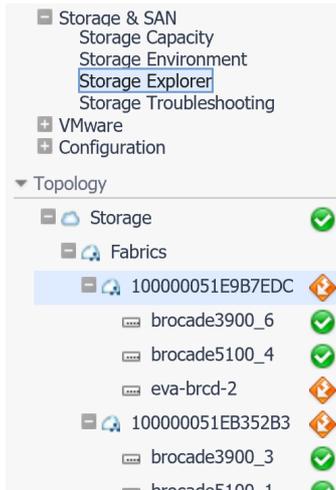
2 On the navigation panel, under Topology, select a storage device. Details about the device and its components are displayed in a Storage Explorer dashboard.

All Storage Explorer dashboards have a similar organization.

Table 19. Storage Explorer dashboards contain the following common screen elements:

Screen Element	Description
Time Range	Displays and controls the period of time represented in the dashboard. The default is the last four hours. For more information, see "Time Range" in the online help.
Alarm Count	Displays counts of all the alarms at each severity level that are still active (not cleared) at the end of the displayed time range. Unlike the Alarm Summary view, the Alarm Count includes alarms for the device and all its child components. Click an alarm count to display the alarms at that severity level.

Table 19. Storage Explorer dashboards contain the following common screen elements:

Screen Element	Description
Summary Tab Views	When the Summary tab is selected: • The top view displays the same Related Inventory view and charts that are displayed for this device in the Storage Environment quick view. • The Summary and Resource Information view displays physical configuration details for the selected device. • The Alarm Summary displays device-level alarms (if any).
Component Tabs	Contains a tab for each type of component used by the selected device, such as ports, drives, and disks. When a component tab is selected: • The top view displays key performance and/or capacity metrics for the components used by this device. • A Details view lists the components by name and displays physical configuration details. • The Alarm Summary displays component-level alarms (if any). • Other component-specific views may be present.
FAQts Tab	Contains questions appropriate for the selected device type. For information on how to use a FAQts tab, see Asking Questions About the Monitored Storage Environment.
Alarm Summary	Displays alarms for the selected device (on the Summary tab) or the type of component (on the Component tabs).

For information about each type of Storage Explorer dashboard, see the following topics:

- Exploring a Fabric
- Exploring a Switch
- Exploring a Cisco VSAN
- Exploring a Storage Array
- Exploring a Filer

Exploring a Fabric

The Storage Explorer's Fabric dashboard contains information about the selected fabric and its switches as well as all ports used by the switches in the fabric. The data displayed reflects values for the selected time range. This walkthrough describes the contents of each of the tabs and points you to where you can drill down for more details.

To explore a fabric:

1   On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2   On the navigation panel, under Topology, expand **Fabrics** and select a fabric.

The Fabric dashboard opens with details for the selected fabric.

> **i** | **TIP:** You can also open this dashboard from the Storage Environment dashboard by selecting a fabric and clicking View in Explorer.

3   If the Alarm Count displays alarms, you may want to assess the alarms before continuing with this walkthrough. Click a status count to open a list of device and component alarms. For more information, see Assessing Storage Alarms.

4   In the **Summary** tab, review performance in terms of key metrics.

The Summary tab contains the same Related Inventory view and Resource Utilization charts as the Fabric Summary quick view described in Monitoring Fabrics. In addition, the tab includes the following views:

- **Summary and Resource Information**. Displays physical details about the fabric.

- **FC Switch Detail**. For each switch, displays the switch status, type of switch (physical or logical), and current value for Data Rate, followed by details about the ISL ports and N ports belonging to the switch. Ports details include the number of ports by alarm status and current values for Link Error Rate and Non-Link Error Rate. Click a 〰 Sparkline to plot metric values over the time period.

- **Alarm Summary**. Displays alarms on this fabric.

5   Click the **ISL Ports** tab.

- **Highest charts**. The charts display the top three ISL ports in the fabric with the highest average Data Rate, Link Error Rate, and Non-Link Error Rate, respectively. The tables show the average and current values for the ports.
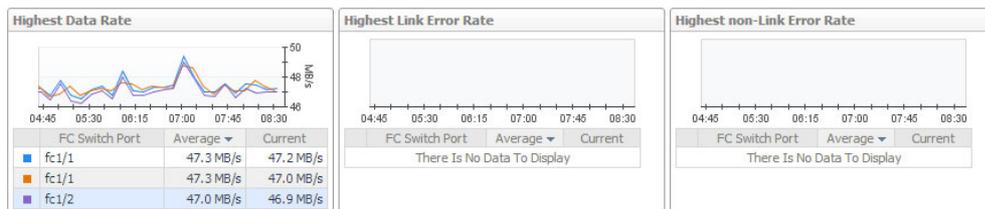
- **Topology Table (Inter-Switch Connections)**. For each switch, identifies all ISL port connections with other switches in the fabric.

- **Port Details**. For each switch-plus-port combination, displays the name and type of switch (physical or logical) and the port name, status, and physical state. The metrics represent current values for Rcvd Utilization, Xmit Utilization, Link Error Rate, Non-Link Error Rate, and Link Speed. Click a 〰 Sparkline to plot metric values over the time period.

    i | **NOTE:** When the selected fabric is a Cisco physical fabric with VSANs, this table includes a VSAN column that identifies the VSANs to which each ISL port is assigned.

You can add the following metrics to the table by clicking the **Customizer** 🔣 icon:
Frame Rate, Data Receive Rate, Data Rate, and Data Send Rate.

- **Alarm Summary**. Displays alarms on ISL ports.

6   Click the **N Ports** tab.

- **Highest charts**. The charts display the top three N ports in the fabric with the highest average Rcvd Utilization, Xmit Utilization, Link Error Rate, and Non-Link Error Rate, respectively. The tables show the average and current values for the ports.

> **i** | **NOTE:** When the selected fabric is a Cisco physical fabric with VSANs, the tables include a VSAN column that identifies the VSAN to which an N port is assigned.
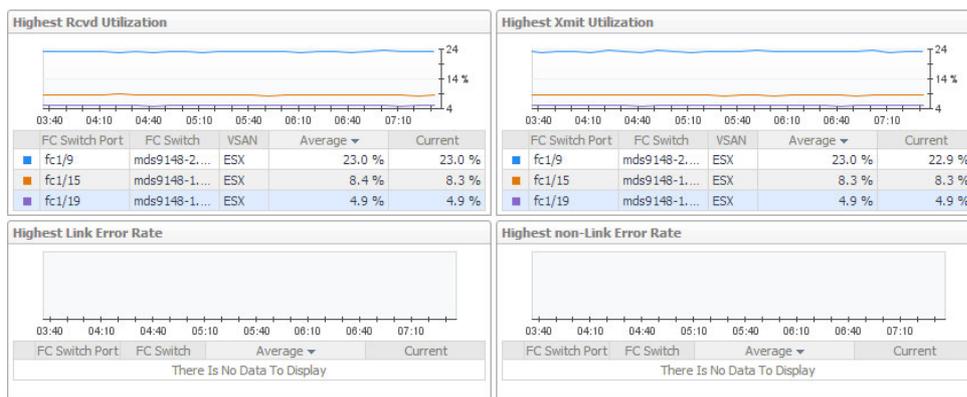
- **Port Details**. For each switch-plus-port combination, displays the name and type of switch and the port name, status, and physical state. The metrics represent current values for Rcvd Utilization, Xmit Utilization, Link Error Rate, Non-Link Error Rate, and Link Speed. Click a 〰️ Sparkline to plot metric values over the time period.

> **i** | **NOTE:** When the selected fabric is a Cisco physical fabric with VSANs, this table includes a VSAN column that identifies the VSAN to which an N port is assigned.

You can add the following metrics to the table by clicking the **Customizer** 🔣 icon:
Frame Rate, Data Receive Rate, Data Rate, and Data Send Rate.

- **Alarm Summary**. Displays alarms on N ports.

7 To investigate further, click the name of a component on any tab:

- Click a switch name. See Exploring a Switch.

- Click a port name. See Investigating an FC Switch Port.

- For Cisco fabrics with VSANs, click the text in the VSAN column and then select a VSAN. See Exploring a Cisco VSAN.

- Click an alarm. See Assessing Storage Alarms.

8 To change the fabric name to a more user-friendly name, click the fabric name in the Summary and Resource Information panel.

The Change Fabric Name dialog appears, allowing you to enter a new name.

Exploring a Switch

The Storage Explorer's FC Switch dashboard contains information about the selected Fibre Channel switch and all ports used by the switch. The data displayed reflects metric values for the selected time range. This walkthrough describes the contents of each of the tabs and points you to where you can drill down for more details.

To explore a switch:

1 On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2 On the navigation panel, under Topology, expand **Fabrics**, expand the target fabric, and select a switch.

The FC Switch dashboard opens with details for the selected switch.

> **i** | **TIP:** You can also open this dashboard from the Storage Environment dashboard by selecting a switch and clicking View in Explorer.

3 If the Alarm Count displays alarms, you may want to assess the alarms before continuing with this walkthrough. Click a status count to open a list of device and component alarms. For more information, see Assessing Storage Alarms.

4 In the **Summary** tab, review performance in terms of key metrics.

The Summary tab contains the same Related Inventory view and Resource Utilization charts as the FC Switch Summary quick view described in Monitoring Fabrics. In addition, the tab includes the following views:

- **Summary and Resource Information**. Displays physical details about the switch.

- **Topology Table (Inter-Switch Connections)**. *Brocade logical switches only.* For each switch, identifies all ISL port connections with other switches in the fabric.

- **Alarm Summary**. Displays alarms on the switch.

5 Click the **ISL Ports** tab, if available.

> **i** | **NOTE:** This tab is hidden when the switch is a Brocade logical switch that uses only logical ISL ports for inter-switch connections. No metrics are available for logical ISL ports. The Topology Table (Inter-Switch Connections) table appears on the Summary tab instead.

Displays the same information as the ISL Ports tab on the Fabric dashboard, but the data reflects only the ISL ports used by the selected switch. For more information, see Exploring a Fabric.

6 Click the **N Ports** tab.

Displays the same information as the N Ports tab on the Fabric dashboard, but the data reflects only the N ports used by the selected switch. For more information, see Exploring a Fabric.

7 To investigate further, click the name of a component on any tab:

- Click a port name. See Investigating an FC Switch Port.

- For Cisco fabrics with VSANs, click the text in the VSAN column and then select a VSAN. See Exploring a Cisco VSAN.

- Click an alarm. See Assessing Storage Alarms.

Exploring a Cisco VSAN

The Storage Explorer's VSAN dashboard contains information about the selected Cisco VSAN and all ports that are part of the VSAN. The data displayed reflects metric values for the selected time range. This walkthrough describes the contents of each of the tabs and points you to where you can drill down for more details.

To explore a VSAN:

1   On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2   On the navigation panel, under Topology, expand **Fabrics**, expand a Cisco fabric with VSANs, and select a VSAN.

The VSAN dashboard opens with details for the selected VSAN.

> **i** | **TIP:** You can also open this dashboard from the Storage Environment dashboard by selecting a VSAN and clicking View in Explorer.

3   If the Alarm Count displays alarms, you may want to assess the alarms before continuing with this walkthrough. Click a status count to open a list of device and component alarms. For more information, see Assessing Storage Alarms.

4   In the **Summary** tab, review performance in terms of key metrics.

The Summary tab contains the same Related Inventory view and Resource Utilization charts as the VSAN Summary quick view described in Monitoring Fabrics.

5   Click the **ISL Ports** tab.

Displays the same information as the ISL Ports tab on the Fabric dashboard, but the data reflects only the ports that are part of the selected VSAN. For more information, see Exploring a Fabric.

6   Click the **N Ports** tab.

Displays the same information as the N Ports tab on the Fabric dashboard, but the data reflects only the ports that are part of the selected VSAN. For more information, see Exploring a Fabric.

7   To investigate further, click the name of a component on any tab:

- Click a port name. See Investigating an FC Switch Port.

- Click an alarm. See Assessing Storage Alarms.

Exploring a Filer

Foglight for Storage Management supports NetApp filers. NetApp uses the word *aggregate* instead of pool, but the metrics collected for aggregates and pools are similar. In some filer views, in particular the views on the LUNs tab and Disks tabs, the word pool may be displayed instead of aggregate, but in this context it refers to aggregates.

The Storage Explorer's Filer dashboard contains information about the selected filer and its child components. The data displayed reflects values for the selected time range. This walkthrough describes the contents of each of the tabs and points you to where you can drill down for more details.

To explore a filer:

1   On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2   On the navigation panel, under Topology, expand **Filers** and select a filer.

The Filer dashboard opens with details for the selected filer.

> **i** │ **TIP:** You can also open this dashboard from the Storage Environment dashboard by selecting a filer and clicking View in Explorer.

3   In the **Summary** tab, review performance in terms of key metrics.

The Summary tab contains the same views as the Filer Summary (Selected Filer) quick view described in Monitoring Filers. In addition, the tab includes the following views:

- **Summary and Resource Information**. Displays physical details about the filer.
- **Alarm Summary**. Displays alarms on the filer.

4   Click the **Controllers-Ports** tab.

- **Controllers**. The charts display the controllers with the highest average Data Rate and Ops Rate. The table displays current values for each of the charted metrics, plus Latency by block and file and the most severe alarm status on the FC ports and IP ports associated with this controller.
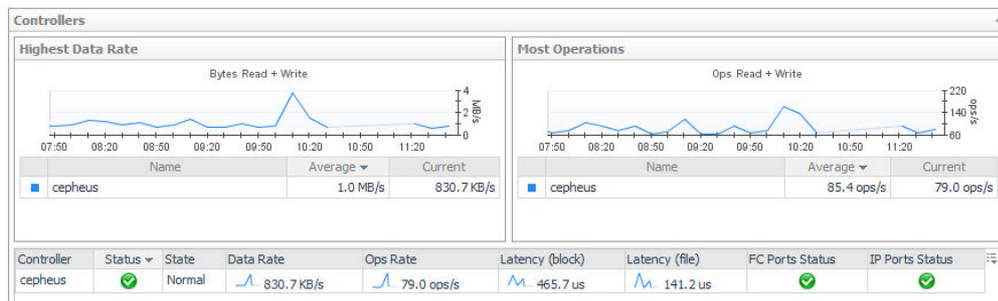
- **Ports**. Select a controller from the **Show Ports for Controller** list. The ports associated with the selected controller are displayed, however the port's physical state and performance metrics are unavailable for NetApp filers. The IP ports shown are used for iSCSI I/O to LUNs traffic.
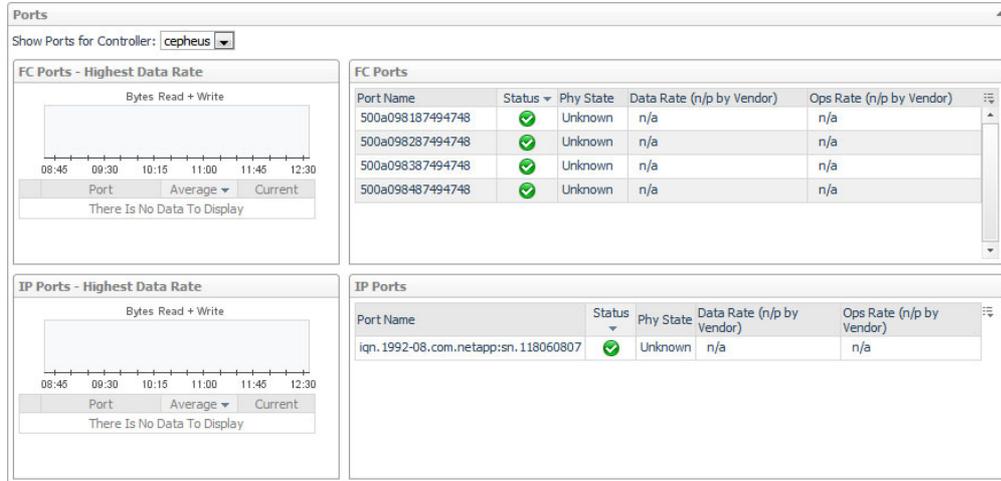
- **Alarm Summary**. Displays alarms on controllers and ports.

5   To investigate further, click the name of a component:

- Click a controller name. See Investigating a Controller.
- Click a port name. See Investigating an Array/Filer Port.
- Click an alarm. See Assessing Storage Alarms.

6   Click the **Aggregates** tab.

- **Lowest Available Capacity**. Displays the five aggregates with the lowest average value for Available Usable Capacity over the time period.

- **Most Overcommitted Aggregates**. Identifies up to five of the most overcommitted aggregates, and displays current values for Advertised NASVolumes Size, Total Usable Capacity, and Used Capacity.
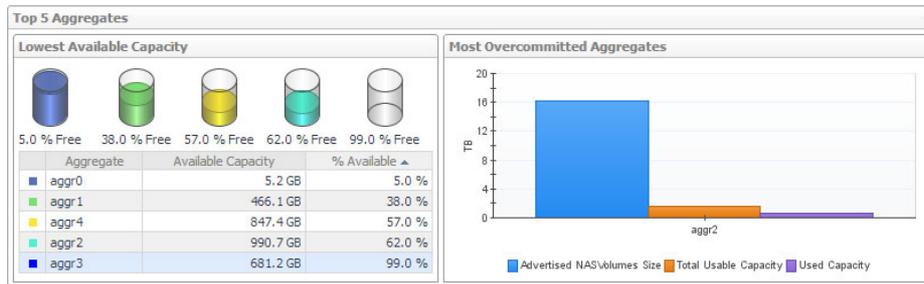
- **Aggregate Details**. For each aggregate, displays the aggregate name, status, and current values for Total Usable Capacity, Available Usable Capacity, % Available, Advertised NASVolumes Size, and Overcommitment.

- **Alarm Summary**. Displays alarms on aggregates.

  To investigate further, click the name of a component:

  - Click an aggregate name. See Investigating an Aggregate.
  - Click an alarm. See Assessing Storage Alarms.

7   Click the **NASVolumes** tab.

This view lets you quickly see the top 15 NASVolumes with a selected metric, averaged over the selected time period.

Selecting the time period "for current" shows the NASVolumes with the worst current metric.

Selecting the time period "last 30 minutes, last hour, last 4 hours" shows the NASVolumes with the worst average values in that time period.

> **i** | **NOTE:** The selected time range looks at the average of values from collections that completed between the time at the end of the zonar, and the selected period before that.

The bars in the Average column show the values of the other items' metric relative to the first (highest) item.

Click on a name in the table, and summary details about that item will be displayed in details panel below. This panel will display the exact time period of the completed collections in the selected timerange.

To further investigate the selected item, click **Explore** in the details panel. See Investigating a NASVolume.

- Alarm Summary. Displays alarms on NASVolumes.

  To investigate further, click an alarm. See Assessing Storage Alarms.

8 Click the LUNs tab.

9 Click the Disks tab.

> **i** | **NOTE:** To investigate a NASVolume, LUN, or Disk that is not included in the Top 15 items on the NASVolumes, LUNs, or Disks tab, use the Advanced Find functionality on the Advanced Find tab to query for the desired items. For more information, see Advanced Find.

Exploring a Storage Array

The Storage Explorer's Storage Array dashboard contains information about the selected storage array and its child components.

The tabs displayed on the dashboard differ depending on the selected storage array:

- Non-Clustered Storage Arrays (supported storage arrays except EqualLogic and Isilon)
- Dell EqualLogic Storage Array
- EMC Isilon Storage Array
- EMC VPLEX Storage Array

Non-Clustered Storage Arrays

Most supported storage arrays are displayed as described in this walkthrough. If you are using Dell EqualLogic arrays, EMC Isilon arrays, or EMC VPLEX arrays, see Dell EqualLogic Storage Array, EMC Isilon Storage Array, or EMC VPLEX Storage Array instead.

This walkthrough describes the contents of each of the tabs and points you to where you can drill down for more details. The data displayed reflects values for the selected time range.

To explore storage arrays:

1 On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2 On the navigation panel, under Topology, expand **Storage Arrays** and select a storage array.

The Storage Array dashboard opens with details for the selected storage array.

> **i** | **TIP:** You can also open this dashboard from the Storage Environment dashboard by selecting an EqualLogic storage array and clicking View in Explorer.

3   If the Alarm Count displays alarms, you may want to assess the alarms before continuing with this walkthrough. Click a status count to open a list of device and component alarms. For more information, see Assessing Storage Alarms.

4   In the **Summary** tab, review performance in terms of key metrics.

The Summary tab contains the same views as the Storage Array Summary (*Selected Storage Array*) quick view described in Monitoring Storage Arrays. In addition, the tab includes the following views:

- **Summary and Resource Information**. Displays physical details about the storage array.

- **Alarm Summary**. Displays alarms on the storage array.

5   Click the **Controllers-Ports** tab.

- **Controllers**. The charts display the controllers with the highest average Data Rate, Ops Rate, and % Busy, if available. The table displays current values for each of the charted metrics, plus Latency if available, and the most severe alarm status on the FC ports and IP ports associated with this controller.

- **Ports**. Select a controller from the **Show Ports for Controller** list. The chart will display port utilization distribution, if the array provides the operating link speed of the ports. Otherwise, the Data Rate of the 3 busiest ports will be displayed. The tables will display all available current metrics for each port.
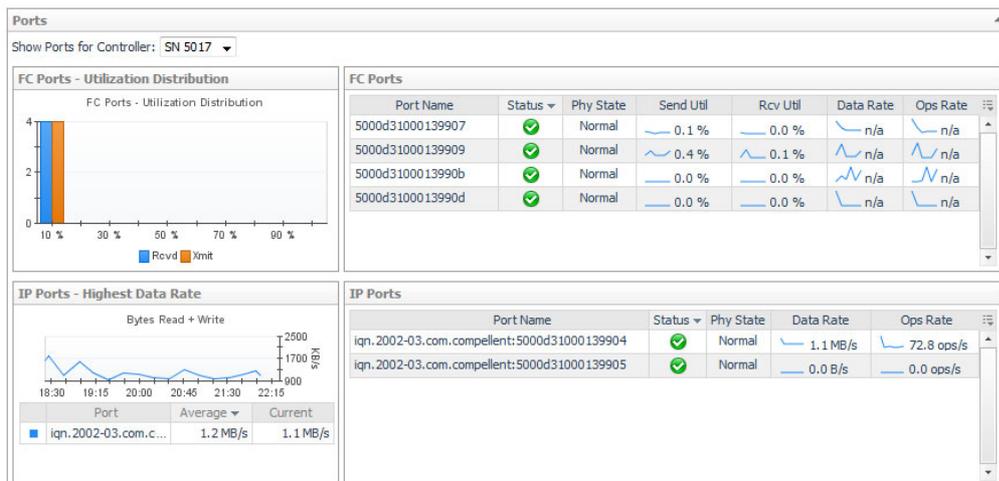
Alarm Summary. Displays alarms on controllers and ports.

To investigate further, click the name of a component:

▫   Click an aggregate name. See Investigating an Aggregate.

▫ Click an alarm. See Assessing Storage Alarms.

6 Click the **Pools** tab.

- **Show Top 15/All Pools/Pools w Thin LUNs With …** This view lets you quickly see the top fifteen or all LUNs with a selected metric, averaged over the selected time period. The performance metrics that may be available for selection, depending on the array type, include:

    ▫ R/w latency

    ▫ Average queue depth

    ▫ Data rate

    ▫ Ops rate to disk

  The capacity metrics that may be available for selection, depending on the array type, include:

    ▫ Least time until full

    ▫ Least or most available usable capacity

    ▫ Least or most available raw capacity

  Selecting the time period "for current" shows the LUNs with the worst current metric.

  Selecting the time period "last 30 minutes, last hour, last 4 hours" shows the LUNs with the worst average values in that time period. These time periods are available only for performance metrics.

  i | **NOTE:** The selected timerange looks at the average of values from collections that completed between the time at the end of the zonar, and the selected period before that.

  The bars in the Average column show the values of the other items' metric relative to the first (highest) item.

  i | **NOTE:** Selecting **Pools w Thin LUNs** is useful for monitoring Pools whose available capacity can change quickly because it contains thin-provisioned LUNs.

  Click on a name in the table to display summary details about that item in the details panel below. This panel displays the exact time period of the completed collections in the selected timerange.

  i | **NOTE:** For Hitachi USP and VSP arrays, only user created Dynamic Provisioning (DP) pools are monitored.

  To further investigate the selected item, click "Explore" in the details panel.

- **Alarm Summary**. Displays alarms on pools.

To investigate further, click an alarm. See Assessing Storage Alarms.

7   Click the LUNs tab.

8   Click the Disks tab.

9   Click the **Advanced Find** tab to investigate a LUN or Disk that is not included in the Top 15 items on the LUNs or Disks. Use the Advanced Find functionality to query for the desired items. For more information, see Advanced Find.

Dell EqualLogic Storage Array

Foglight for Storage Management monitors Dell EqualLogic array groups. In the interface, groups are categorized as Storage Arrays, and array members are called *Member Nodes* or simply *Members*.

This walkthrough describes the contents of each of the tabs and points you to where you can drill down for more details. The data displayed reflects values for the selected time range.

To explore an EqualLogic storage array:

1   On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2   On the navigation panel, under Topology, expand **Storage Arrays** and select an EqualLogic group.

The Storage Array dashboard opens with details for the selected EqualLogic group.

> **i** | **TIP:** You can also open this dashboard from the Storage Environment dashboard by selecting a storage array and clicking View in Explorer.

3   If the Alarm Count displays alarms, you may want to assess the alarms before continuing with this walkthrough. Click a status count to open a list of device and component alarms. For more information, see Assessing Storage Alarms.

4   In the **Summary** tab, review performance in terms of key metrics.

The Storage Explorer's Summary tab contains the same views as the Storage Environment's quick view for EqualLogic storage arrays:

- **Related Inventory**. Contains alarm summaries for the selected storage array and its member nodes, IP ports, pools, LUNs, and disks.

- **Storage Capacity Summary**. Displays current values for Total Advertised LUNs Size and Capacity Provisioned to LUNs.

- **Network Ports Utilization**. Plots aggregated current values for Send Util and Rcv Util over the time period.

- Pools with Severe or High Pressure on Available Usable Capacity:

    □   Displays the pools that have the most significant, near-term capacity issues.

    □   Shows the available usable capacity in the table, the % available, and over commitment.

    □   Shows the estimated time when the pool capacity will be full, if available.

    □   The cylinders are colored to show the % of available capacity in the pool.

- **LUNs/Disks States**. Plots the percentage of disks and LUNs in the storage array in problem states. Problem states are reported by the vendor. Resolving these issues may improve LUN performance.
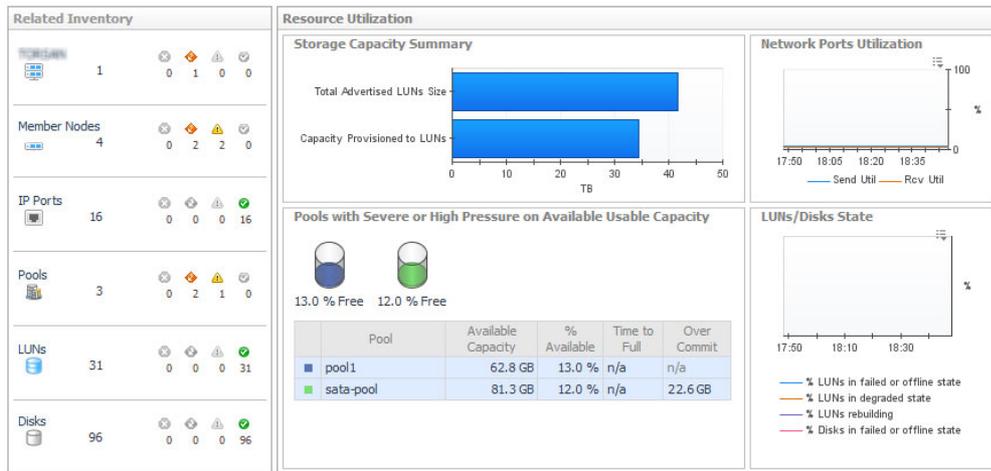
In addition, the tab includes the following views:

- **Summary and Resource Information**. Displays physical details about the storage array.

- **Alarm Summary**. Displays alarms on the storage array.

5   Click the **Network** tab.

- **Network Summary**. Identifies the load on the network, in terms of Send Util and Rcv Util, and the Packet Errors % over the time period.
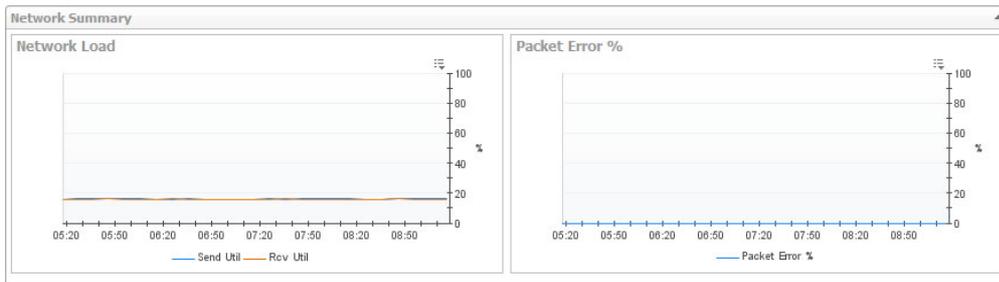
- **Port Status Filter**. Click to show only ports with the selected status in the Port Details table.

- **Port Details**. For each member-plus-port combination, displays current values for Data Rate, Send Util, Rcv Util, Packet Errors %, and Link Speed. Click a 〜 Sparkline to plot metric values over the time period. Also displays the member's IPv4 and IPv6 addresses, if available.

- **Alarm Summary**. Displays alarms on ports.

6   Click the **Pools-Members** tab.

- **Highest charts**. Display the pools with the highest average value for Ops Rate and Latency. Also shows aggregated values for Total Advertised LUNs Size and Capacity Provisioned to LUNs for all members.
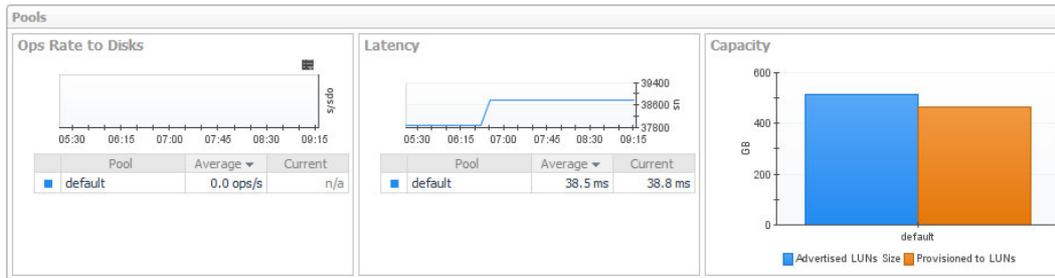
- **Pool Details**. For each pool, displays its name, status, and current values for Data Rate, Ops Rate, Latency, Average Queue Depth, Total Advertised LUNs Size, Total Usable Capacity, Available Usable Capacity, Capacity Provisioned to LUNs, and Overcommitment. Click a 〰 Sparkline to plot metric values over the time period. Also identifies pool members.

- **Member Details**. For each member, displays its name, parent pool, status, and current values for Data Rate, Ops Rate, Latency, Send Util, Rcv Util, Total Usable Capacity, % Used, and % of Pool. Also displays the RAID level in use for the member.

- **Alarm Summary**. Displays alarms on pools and members.

7 Click the LUNs tab.

8 Click the Disks tab.

9 To investigate further, click the name of a component on any tab:

   - Click a port name. See Investigating an Array/Filer Port.

   - Click an array member name. See Investigating an EqualLogic Member.

   - Click a pool name. See Investigating a Pool.

   - Click an alarm. See Assessing Storage Alarms.

10 Click the **Advanced Find** tab to investigate a LUN or Disk that is not included in the Top 15 items on the LUNs or Disks. Use the Advanced Find functionality to query for the desired items. For more information, see Advanced Find.

EMC VPLEX Storage Array

Foglight for Storage Management monitors EMC VPLEX clusters. In the interface, clusters are categorized as *VPLEX Clusters*.

This walkthrough describes the contents of each of the tabs and points you to where you can drill down for more details. The data displayed reflects values for the selected time range.

To explore a VPLEX storage array:

1 On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2 On the navigation panel, under Topology, expand **VPLEX Clusters** and select a VPLEX cluster.

   The Clusters dashboard opens with details for the selected VPLEX cluster.

i | **TIP:** You can also open this dashboard from the Storage Environment >Virtualization dashboard by selecting an VPLEX storage array and clicking View in Explorer.

3   If the Alarm Count displays alarms, you may want to assess the alarms before continuing with this walkthrough. Click a status count to open a list of device and component alarms. For more information, see Assessing Storage Alarms.

4   In the **Summary** tab, review performance in terms of key metrics.

The Storage Explorer's Summary tab contains the same views as the Storage Environment's quick view for VPLEX storage arrays:

- **Related Inventory**. Contains alarm summaries for the selected cluster and its directors, frontend ports, backend ports, virtual volumes, storage volumes, storage arrays, and fabrics.

- **Top directors charts.** Lists top 3 directors by CPU usage, Heap Usage, Data Rate and Ops.

- **Engine Information**. Displays physical details about the VPLEX array.

- **Alarm Summary**. Displays alarms on the VPLEX array.

5   Click the **Storage Volumes** tab.

- **Top 5 Storage Volumes**. Lists top 5 storage volumes of highest average latency.

- **Storage Volumes Status Filter**: Click to show only storage volumes with the selected status in the Storage Volumes Detail table.

- **Storage Volumes Detail** table. For each storage volume, displays its name, status, IO status, Operational Status, Source, Capacity, Latency, and LUN used by this storage volume.

- **Alarm Summary**. Displays alarms on the Storage Volume.

- To investigate further, see Investigating a Storage Volume on page 147.

6   Click the **Directors - Ports** tab.

- **Top 3 Directors**. Displays the top three back-end/front-end directors with the highest average value for Data Rate, Operations, and Errors. The charts plot values over the time period, while the tables show the average and current values for each director.

- **Top 3 Ports.** Displays the top three back-end/front-end ports with the highest read and writer bytes. The charts plot values over the time period, while the tables show the average and current values for each port.

- Backend Ports table for each director.

- Frontend Ports table for each director.

- **Alarm Summary**. Displays alarms on directors.

- To investigate further, see Investigating Director - Ports on page 145.

7   Click the **Virtual Volumes** tab.

- **Top 5 Virtual Volumes**. Displays the top five virtual volumes by Data Rate, Average Latency and Ops Rate.

- **Virtual Volumes Status Filter**: Click to show only virtual volumes with the selected status in the Virtual Volumes Detail table.

- **Virtual Volumes Detail** table. For each virtual volume, displays its name, status, Operational State, Health State, Supporting Device, Latency, Data Rate, Ops Rate, and Capacity.

- **Alarm Summary**. Displays alarms on virtual volumes.

- To investigate further, see Investigating a Storage Volume on page 147.

EMC Isilon Storage Array

Foglight for Storage Management monitors EMC Isilon clusters. In the interface, clusters are categorized as *Storage Arrays*, and the nodes are called *Member Nodes* or simply *Members*.

This walkthrough describes the contents of each of the tabs and points you to where you can drill down for more details. The data displayed reflects values for the selected time range.

To explore an Isilon storage array:

1 On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2 On the navigation panel, under Topology, expand **Storage Arrays** and select an Isilon cluster.

   The Storage Array dashboard opens with details for the selected Isilon cluster.

   > **i** | **TIP:** You can also open this dashboard from the Storage Environment dashboard by selecting an Isilon storage array and clicking View in Explorer.

3 If the Alarm Count displays alarms, you may want to assess the alarms before continuing with this walkthrough. Click a status count to open a list of device and component alarms. For more information, see Assessing Storage Alarms.

4 In the **Summary** tab, review performance in terms of key metrics.

   The Storage Explorer's Summary tab contains the same views as the Storage Environment's quick view for Isilon storage arrays:

   - **Related Inventory**. Contains alarm summaries for the selected storage array and its member nodes, external ports, internal ports, pools, and disks.

   - **IFS Capacity**. The chart displays IFS Capacity: Free and IFS Capacity Used for the IFS file system. In addition, the following metrics pairs are displayed:

     - IFS Capacity: Total and IFS Capacity: Free
     - IFS Capacity: HDD Total and IFS Capacity: HDD Free
     - IFS Capacity: SDD Total and IFS Capacity: SDD Free

   - **Average CPU Busy %**. Displays the aggregate value of % Busy for all nodes in the array over the time period.

   - **File System Throughput**. Plots Data Read Rate and Data Write Rate to the file system over the time period.

   - **Disk System Throughput**. Plots Data Read Rate and Data Write Rate to the disk over the time period.

   - **External Network Throughput**. Plots the Rcv Data Rate and Send Data Rate for the external network over the time period.

   > **i** | **TIP:** If you prefer to see the Send Util (% of max) and Rcv Util (% of max) based on the rated maximum speeds of the ports (actual port speeds are not available from Isilon arrays) in the external network, ask your Foglight for Storage Management Administrator to edit the registry variable *StSAN_StoragePortShowUtilMax* and set `ISLN_E_IP=true`.

   - **Internal Network Throughput**. Plots the Rcv Data Rate and Send Data Rate for the internal network over the time period.

   - **Clients**. Plots clients connected versus clients that are actively using the network over the time period.
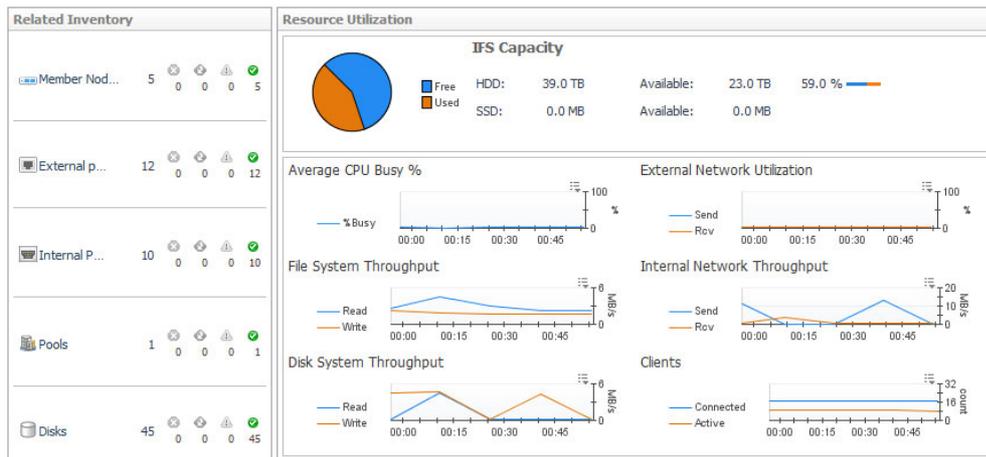
In addition, the tab includes the following views:

- **Summary and Resource Information**. Displays physical details about the storage array.
- **Alarm Summary**. Displays alarms on the storage array.

5. Click the **Network** tab.

Use this tab to understand network utilization and packet errors by port.

External Network Summary

- **Charts**. Plot aggregated values for Send Data Rate and Rcv Data Rate, and Packet Errors % for the external network connections over the time period.
- **Port Status Filter**. Click this link to show only ports with a selected status in the Port Details table.
- **Port Details**. For each port used by the external network, identifies the port name, parent node, status, physical state, and current values for Send Data Rate, Rcv Data Rate, and Packet Errors %. Also displays the maximum speed of the port. Click a ∿ Sparkline to plot metric values over the time period.

> **i** | **NOTE:** When the registry variable *StSAN_StoragePortShowUtilMax* is set to show port utilization, this table also displays Rcv Util and Send Util.

- **Alarm Summar**y. Displays alarms on ports used by the external network.
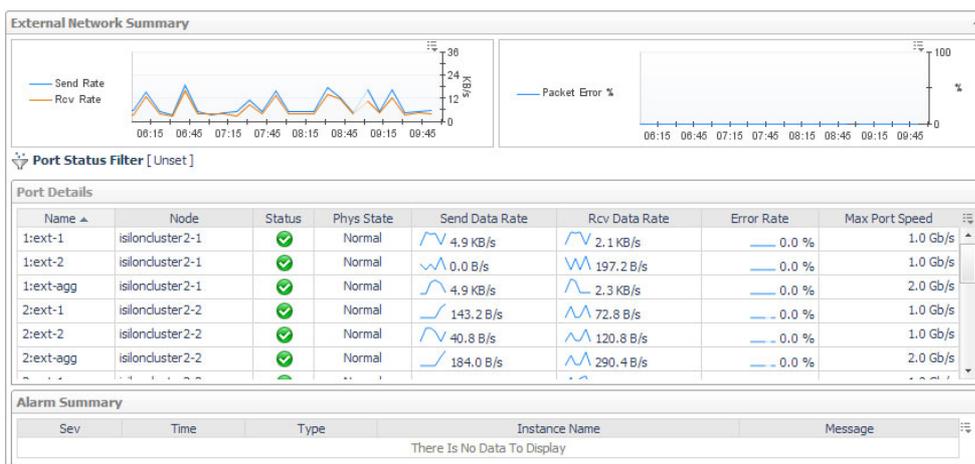
Internal Network Summary

- **Charts**. Plot aggregated values for Send Data Rate, Rcv Data Rate, and Packet Errors % for the internal network connections over the time period.

- **Port Status Filter**. Click this link to show only ports with a selected status in the Port Details table.

- **Port Details**. For each port used by the internal network, identifies the port name, parent node, status, physical state, and current values for Send Data Rate, Rcv Data Rate, and Packet Errors %. Also displays the maximum speed of the port. Click a ⌁ Sparkline to plot metric values over the time period.

> **i** | **NOTE:** When the registry variable *StSAN_StoragePortShowUtilMax* is set to show port utilization, this table can also display Rcv Util and Send Util.

- **Alarm Summar**y. Displays alarms on the external network and its ports.

6   Click the **Member Nodes** tab.

- **Top 5 Nodes**. Displays the top five member nodes with the highest average value for Data Rate, Latency, and % Busy. The charts plot values over the time period, while the tables show the average and current values for each node.
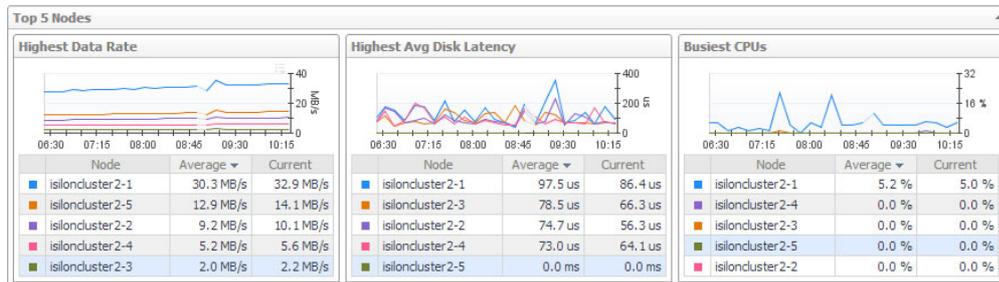
- **Node Status Filter**. Click to show only member nodes with the selected status in the Node Details table.

- **Node Details**. For each member node, displays its name, status, physical state, and current values for Data Rate, % Busy, Latency, L2 Cache Hit Rate, IFS Capacity, and IFS Capacity: Free. Also displays the worst status of the node's disks, external network ports, and internal network ports, and identifies the node's parent pool. Click a ⌁ Sparkline to plot metric values over the time period.

You can add the following metrics to the table by clicking the **Customizer** ⊞ icon: L1 Cache Hit Rate, Send Data Rate and Rcv Data Rate. You can also choose to display other Isilon details, such as Total Disk IOPS and Model.

- **Alarm Summary**. Displays alarms on nodes.

7   Click the **Pools** tab.

- **Top 5 Pools**. Displays the top five pools with the highest average value for Data Rate and Latency, and the lowest average value for L2 Cache Hit Rate. The charts plot values over the time period, while the tables show the average and current values for each pool.
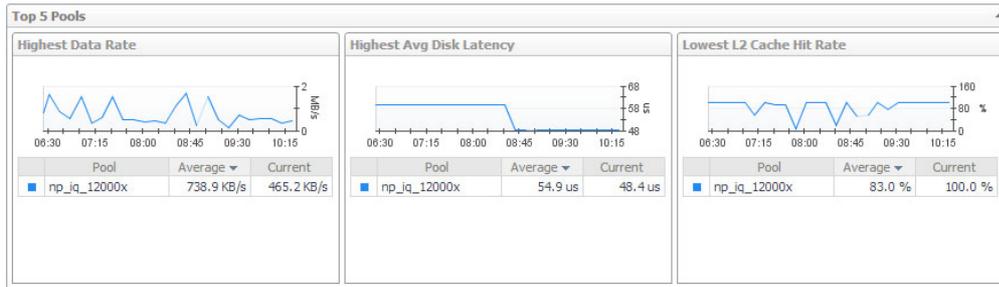
- **Pool Status Filter**. Click to show only pools with the selected status in the Pool Details table.

- **Pool Details**. For each pool, displays its name, status, and current values for Data Rate, Latency, L2 Cache Hit Rate, IFS Capacity, IFS Capacity: Free, HDD % Free, and SDD % Free. Also displays the tier that the pool belongs to and the worst status of nodes associated with the pool. Click a ⌇ Sparkline to plot metric values over the time period.

You can add the following metrics to the table by clicking the **Customizer** ⊞ icon: Ops Rate, % Busy, and L1 Cache Hit Rate.

- **Alarm Summary**. Displays alarms on pools.

8 Click the **IFS** tab.

- **Current Capacity Usage**. For each pool or tier, displays the following sets of metrics:

  - IFS Capacity: HDD Total, IFS Capacity: HDD Used, IFS Capacity: HDD Free, and HDD % Free
  - IFS Capacity: SDD Total, IFS Capacity: SDD Used, IFS Capacity: SDD Free, and SDD % Free

- **File System**. Plots Data Read Rate and Data Write Rate values and Read Ops Rate and Write Ops Rate values for the file system over the time period.
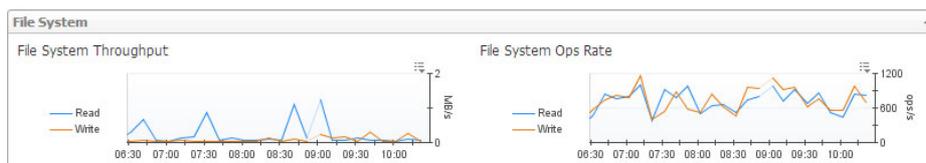
- **Exported Directories**. For each exported directory, states whether the directory is used in the monitored environment. When *Used=true*, you can click the directory name to view a topology diagram showing the datastores that mount the directory

9   Click the Disks tab.

10 To investigate further, click the name of a component on any tab:

- Click a port name. See Investigating an Array/Filer Port.

- Click a member node name. See Investigating an Isilon Node.

- Click a pool name. See Investigating a Pool.

- When a directory is used in the monitored environment, click the directory name. See Investigating a Directory.

- Click an alarm. See Assessing Storage Alarms.

11 Click the **Advanced Find** tab to investigate a Disk that is not included in the Top 15 items on the Disks. Use the Advanced Find functionality to query for the desired items. For more information, see Advanced Find.

Common Data for Filers and Storage Arrays

LUNs tab

A LUN (logical unit) is the block storage element made available by an array or filer to a server.

- **Show LUNs With …**

  This view lets you quickly see the top 15 LUNs with a selected metric, averaged over the selected time period.

  - Selecting the time period "for current" shows the LUNs with the worst current metric.

  - Selecting the time period "last 30 minutes, last hour, last 4 hours" shows the LUNs with the worst average values in that time period.

  > **i** | **NOTE:** The selected time range looks at the average of values from collections that completed between the time at the end of the zonar, and the selected period before that.

The bars in the Average column show the values of the other items' metric relative to the first (highest) item.

Show LUNs With	Highest average r/w latency ▾	for last hour ▾						
		Average Latency for last hour			Other metrics for last hour			
Name	Pools/Parity Groups	Average	Average	Current	Ops Rate	Data Rate	% Busy	
🗄 LUN 94_ds5	Raid Group 0		199.5 ms	299.5 ms	0.0 ops/s	73.6 B/s	0.0 %	
🗄 Thin LUN 83_ds7	Pool Thin Pool 0 ><&		59.6 ms	52.8 ms	4.6 ops/s	51.2 KB/s	4.5 %	
🗄 LUN 110	Raid Group 0		52.4 ms	54.5 ms	0.0 ops/s	0.0 B/s	0.0 %	
🗄 LUN 93_ds6	Raid Group 0		42.6 ms	38.0 ms	3.6 ops/s	35.0 KB/s	4.0 %	
🗄 Thin LUN 81_ds5	Pool Thin Pool 0 ><&		29.7 ms	30.9 ms	0.0 ops/s	0.0 B/s	0.0 %	
🗄 LUN2_NU_DS2	Pool Thin Pool 0 ><&		24.3 ms	25.2 ms	0.0 ops/s	0.0 B/s	0.0 %	
🗄 LUN 95_ds5	Raid Group 0		22.7 ms	25.0 ms	0.1 ops/s	422.1 B/s	0.0 %	
🗄 LUN4_NU_DS4	Pool Thin Pool 0 ><&		17.1 ms	12.5 ms	0.9 ops/s	5.3 KB/s	0.0 %	
🗄 LUN3_PHI_DS3	Pool Thin Pool 0 ><&		8.6 ms	9.1 ms	0.0 ops/s	0.0 B/s	0.0 %	
🗄 LUN1_NU_DS1	Raid Group 0		7.6 ms	5.5 ms	0.1 ops/s	1.6 KB/s	0.0 %	
🗄 Thin LUN 82_ds6	Pool Thin Pool 0 ><&		6.1 ms	1.8 ms	0.4 ops/s	1.9 KB/s	0.0 %	
🗄 LUN6_OMEGA_DS6	Pool Thin Pool 0 ><&		4.2 ms	4.2 ms	0.1 ops/s	1.6 KB/s	0.0 %	
🗄 LUN4_PHI_DS5	Pool Thin Pool 0 ><&		4.1 ms	4.3 ms	0.0 ops/s	0.0 B/s	0.0 %	

> ℹ **NOTE:** The metrics available in the drop down for selection include only the metrics made available by that particular array or filer vendor.

Click on a name in the table, and summary details about that item will be displayed in details panel below. This panel will display the exact time period of the completed collections in the selected time range.
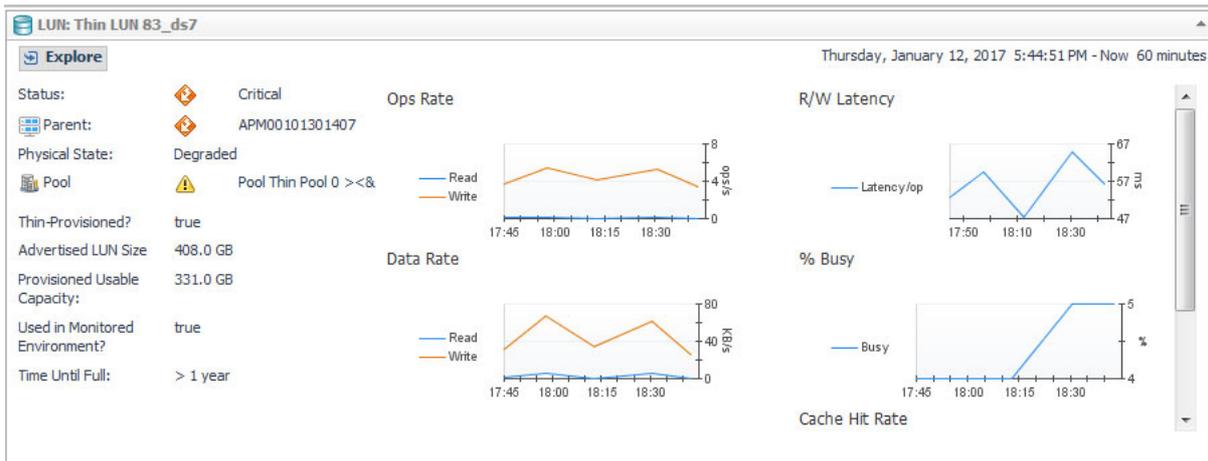
To further investigate the selected LUN, click **Explore** in the details panel. See Investigating a LUN.

- **Alarm Summary**. Displays alarms on LUNs, disks. To investigate further, click an alarm. See Assessing Storage Alarms.

Disks tab

- **Show Disks With...**

This view lets you quickly see the top 15 disks with a selected metric, averaged over the selected time period.

- Selecting the time period "for current" shows the disks with the worst current metric.

- Selecting the time period "last 30 minutes, last hour, last 4 hours" shows the disks with the worst average values in that time period.

  > ℹ **NOTE:** The selected timerange looks at the average of values from collections that completed between the time at the end of the zonar, and the selected period before that.

The bars in the Average column show the values of the other items' metric relative to the first (highest) item.

Show Disks With	Highest average % busy ▾	for selected range ▾				
Name	Pools/Parity Groups	Busy for selected range			Other metrics for selected range	
		Average	Average	Current	Ops Rate	Data Rate
🗄 Bus 0 Enclosure 0 Disk 12	Pool Thin Pool 0 ><&	▬▬▬▬▬▬	2.2 %	0.0 %	7.2 ops/s	137.9 KB/s
🗄 Bus 0 Enclosure 0 Disk 2	Raid Group 0	▬▬▬▬▬▬	2.2 %	1.0 %	6.0 ops/s	479.0 KB/s
🗄 Bus 0 Enclosure 0 Disk 3	Raid Group 0	▬▬▬▬▬	1.8 %	1.0 %	5.9 ops/s	475.8 KB/s
🗄 Bus 0 Enclosure 0 Disk 1	Raid Group 0	▬▬▬▬▬	1.8 %	1.0 %	5.8 ops/s	481.2 KB/s
🗄 Bus 0 Enclosure 0 Disk 0	Raid Group 0	▬▬▬▬▬	1.8 %	1.0 %	5.7 ops/s	480.1 KB/s
🗄 Bus 0 Enclosure 0 Disk 13	Pool Thin Pool 0 ><&	▬▬▬▬	1.5 %	0.0 %	7.2 ops/s	138.4 KB/s
🗄 Bus 0 Enclosure 0 Disk 11	Pool Thin Pool 0 ><&	▬▬▬▬	1.5 %	0.0 %	7.5 ops/s	141.9 KB/s

> **i** | **NOTE:** The metrics available in the drop down for selection include only the metrics made available by that particular array or filer vendor.

Click on a name in the table, and summary details about that item will be displayed in the Details panel below. This panel will display the exact time period of the completed collections in the selected time range
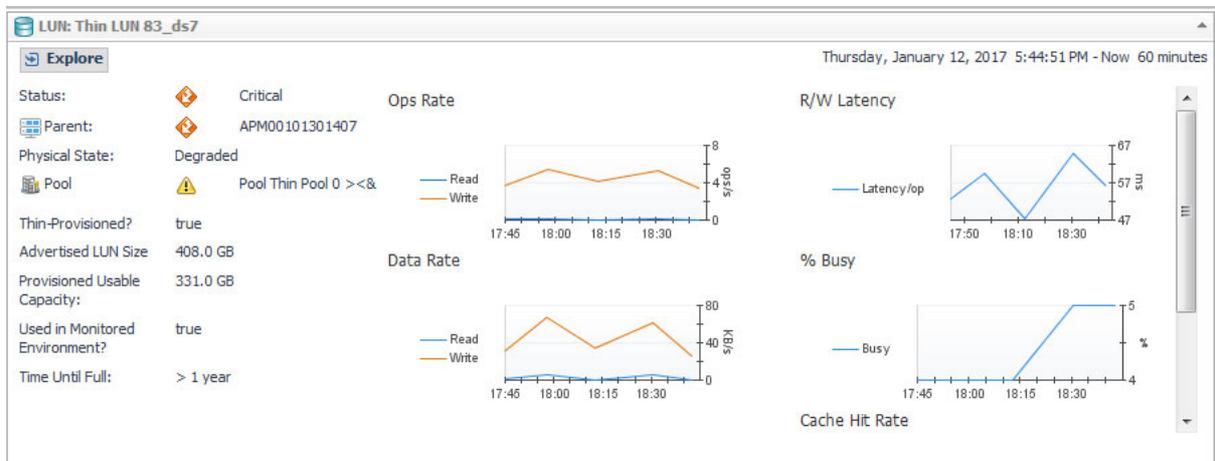
To further investigate the selected disk, click **Explore** in the details panel. See Investigating a Physical Disk.

- **Alarm Summary**. Displays alarms on disks. To investigate further, click an alarm. See Assessing Storage Alarms.

Advanced Find

The tabs for specific entities (like LUNs, Disks, Pools, NASVolumes) quickly identify the Top 15 objects exhibiting the "worst" values for a particular metric. Often, however, there is a need to locate objects by name, or with other characteristics. Use the Advanced Find functionality to locate these items.

Queries can be constructed using a combination of Property conditions and Metric conditions.

Figure 16. Advanced Find

Using the Property Conditions

Finding Entities by Name

To find entities by name:

    1   Select the desired entity type to search for in the Find drop down.

    2   Type the string to search for in the Name Like field.

    3   Click **Perform Query.**

- All items with that string anywhere in their name will be returned.

- _ is a positional wildcard, that can match a single character. For example, `C_D` would match de**cod**e, but would not match `record`

- % is a non-positional wildcard. For example, `C%D` would match re**cord**

Finding Entities with Current Status or Physical State

To find entities with current status or physical state:

    1   Select the desired entity type to search for in the Find drop down.

    2   In Properties, check the status boxes to retrieve entities with that status or state.

    3   Click **Perform Query.**

For example, This example searches for LUNs whose names include a particular string, and have a non-normal alarm state.

The query will take a short time to execute. When it completes, the Latest Query panel will summarize the query conditions. The Query Result panel will display the LUNs found to match the query conditions. The table header displays the time period used for evaluating the query conditions.

Figure 17. Query Conditions

Using the Metric Conditions

The metric conditions area lets you easily construct a more complex query that can include up to 3 conditions on metrics.

Figure 18. Metrics conditions

To use the metric conditions:

1 **Period**. Refers to the time range on the zonar displayed in the upper right-hand corner. Select the time the query should use for the metric values. When *n/a* is selected, this condition is ignored.

2 **Metric**. This drop down shows the metrics available for this entity type for this vendor.

3 The third drop down list provides the comparison operator.

4 Use the fourth field to enter the value to use for the comparison.

5 Use the fifth drop down to select the units for the value you entered. The units selection will change based on the type of metric selected.

6 Click the **+** icon if you want to add another condition. The next condition row will be preceded by a AND/OR selector. A trash can icon will appear to the right of the + icon to let you remove a condition.

Up to 3 conditions can be defined. When the + icon is clicked to display the 3rd condition row, parentheses will be displayed around the first 2 conditions, indicating the order of evaluation.

For example, the following query looks for LUNs that had low average latency during the period, but had a higher latency at the last collection.The query will take a short time to execute. When it completes:

- The Latest Query panel will summarize the query conditions.

- The Query Result panel will display the LUNs found to match the query conditions. The table header displays the time period used for evaluating the query conditions. The metrics used in the query conditions will be displayed in the results table.

To investigate further

  ▫ Click the name of an entity in the table, to drill down to the explorer view for that entity.

  ▫ Click on an alarm Status icon, to display the alarms for that entity.

Investigating Storage Components

To gain a complete picture of the performance of a storage device, you need to understand how its child components are performing.

This section covers the following topics:

- Introducing Storage Component Dashboards
- Investigating an Aggregate
- Investigating an Array/Filer Port
- Investigating a Controller
- Investigating a Directory
- Investigating an EqualLogic Member
- Investigating an FC Switch Port
- Investigating an Isilon Node
- Investigating a LUN
- Investigating a NASVolume
- Investigating a Physical Disk
- Investigating a Pool

Introducing Storage Component Dashboards

A component dashboard is a drill-down view that displays physical details about a selected component, performance and capacity metrics, and alarms. Some also include a topology diagram that shows how the component fits into the monitored environment; for more information, see Exploring Connectivity with SAN Topology Diagrams.

For information about each type of component dashboard, see the following topics:

- Investigating an Aggregate
- Investigating an Array/Filer Port
- Investigating a Controller
- Investigating a Directory
- Investigating an EqualLogic Member
- Investigating an FC Switch Port
- Investigating an Isilon Node
- Investigating a LUN
- Investigating a NASVolume

- Investigating a Physical Disk
- Investigating a Pool

Investigating an Aggregate

The data displayed in the dashboard reflects values for the aggregate over the selected time range. This walkthrough describes the contents of each of the tabs.

To explore an aggregate:

1   On a dashboard, click an aggregate name.

The Aggregate dashboard opens.

2   Review overall performance in the **Summary** tab.

- **Aggregate Details**. Displays the aggregate's status, parent filer, health score, and current values for Advertised NASVolumes Size, Total Usable Capacity, Available Usable Capacity, Overcommitment, Data Rate, and Ops Rate. Click a 〰 Sparkline to plot metric values over the time period.
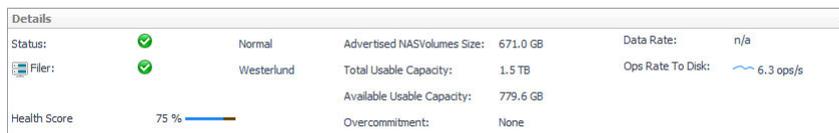
- **Pool Performance**. Displays the same performance metrics found in the Aggregate Details view, but in chart format.
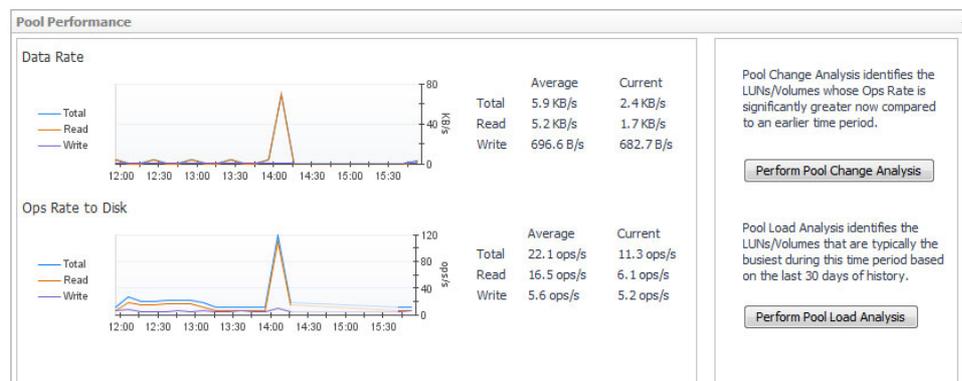
- **Perform Pool Change Analysis**. Click to identify the NASVolumes and LUNs primarily responsible for increased I/O. For more information, see Analyzing the Pool.

- **Perform Pool Load Analysis.** Click to identify the busiest NASVolumes and LUNs, and rank them based on their activity during the same time range *over the last 30 days*. For more information, see Analyzing the Pool.

3   Click the **Capacity** tab.

Displays the following:

- **Capacity Summary**
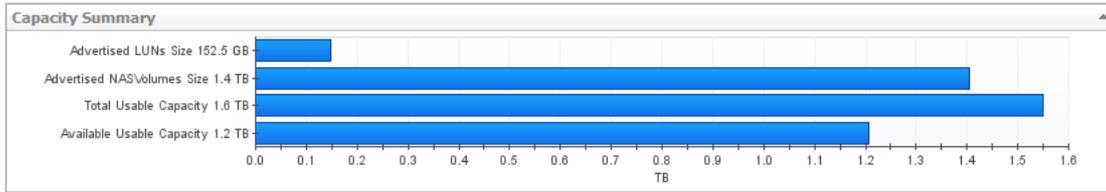
- **Capacity Usage Trends:** Chart provides a visual display of the estimated capacity consumption in the future, based on a regression analysis of the historical capacity consumption.

> **i** | **NOTE:** If time until full shows "n/a", it means enough historical data has not been collected yet. Mouse over to show how much more data is required. For more information, see Capacity Trending.
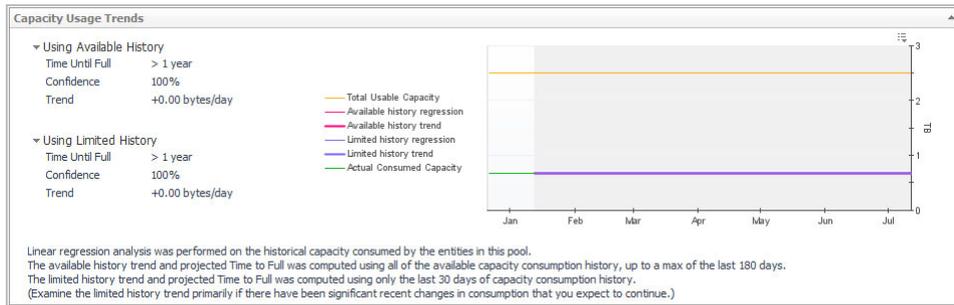
4   Click the **Consumers** tab.

Displays the NASVolumes and LUNs that are configured out of this aggregate.

- **Aggregate Details**. Displays the aggregate's status, parent filer, and current values for Advertised LUNs Size, Advertised NASVolumes Size, Total Usable Capacity, Available Usable Capacity, and Overcommitment.

- **NASVolumes Using This Aggregate**. For each volume, displays its name, status, physical state, and whether the NASVolume is used by an entity in the monitored environment. The metric columns display current values for Data Rate, Latency, Advertised NASVolumes Size, Used Capacity, and % Used. Click a 〰️ Sparkline to plot metric values over the time period.

   The remaining columns provide the following details:
   - **Protection**. Displays the type of protection in use on the volume.
   - **Thin**?. Indicates whether the volume is thin-provisioned (true) or thick-provisioned.
   - **vFiler**. The name of the aggregate's parent virtual filer.

- **LUNs Using This Aggregate.** For each LUN, displays its name, status, physical state, and whether the LUN is used by an entity in the monitored environment. The metric columns display current values for Data Rate, Ops Rate, Latency, % Busy, and Advertised LUNs Size. Click a 〰️ Sparkline to plot metric values over the time period.

   The remaining columns provide the following details:
   - **Protection**. Displays the type of protection in use on the LUN, such as the RAID level.

- **Thin**?. Indicates whether the LUN is thin-provisioned (true) or thick-provisioned.
- **vFiler**. The name of the aggregate's parent virtual filer.

5   Click the **Disks** tab.

Displays the disks used by the selected aggregate. For more information, see Common Component Disk Tab Data.

6   To investigate further:

- Click a NASVolume name. See Investigating a NASVolume (includes a topology diagram).

- Click a LUN name. See Investigating a LUN (includes a topology diagram).

- Click a disk name. See Investigating a Physical Disk.

- Click an alarm. See Assessing Storage Alarms.

Investigating an Array/Filer Port

The data displayed in the dashboard reflects values for the component over the selected time range. This walkthrough describes the contents of each of the tabs.

To explore a port:

1   On a dashboard, click a filer or storage array port.

The Array/Filer Port dashboard opens.

2   Review overall performance in the **Summary** tab.

- **Details**. Displays the port's status, physical details, parent storage array or filer, port controller (for filers and non-cluster arrays) or member node (for cluster arrays), and current values for Data Rate, Ops Rate, Xmit Utilization, and Rcvd Utilization.

- **Charts**. Displays the following metrics over the time period, if available:

- **Data Rate**. Plots values for Data Rate, Data Read Rate, and Data Write Rate.
- **Ops Rate**. Plots values for Ops Rate, Read Ops Rate, and Write Ops Rate.
- **Port Utilization**. Plots values for Send Util and Rcv Util.
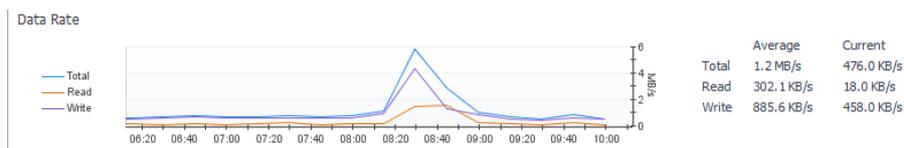
- **Alarm Summary**. Displays alarms on the port.

3   If available, click the **Topology** tab. This tab is displayed for Fibre Channel (FC) ports only.

- **Basic Connectivity (diagram)**. Displays the selected port (left box) and its connection to its controller. If the port is an FC port, the N port on the fibre switch it connects to is also displayed.

- Click an icon for details about the device connected to the port.
- Click a device name to open a list of components that you can drill down on.
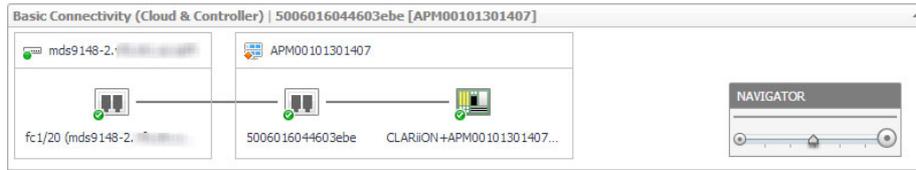
- **Port Dependencies**. On separate tabs, displays connections to LUNs (through the selected port) from virtual machines, ESX or Hyper-V servers, and physical hosts. If the selected port has problems or failures, the connected VMs or hosts may exhibit performance problems.

4 To investigate further:

- In the topology diagram, click a port or controller icon to navigate to related components.

- Click an alarm. See Assessing Storage Alarms.

Investigating a Controller

Controllers manage the ports used by a non-cluster storage array or filer.The data displayed in the dashboard reflects values for the component over the selected time range. The Controller dashboard has two tabs.

To explore a controller and its ports:

1 On a dashboard, click a controller name.

The Controller dashboard opens.

2 Review overall performance in the **Summary** tab.

- **Controller Details**. Displays the controller's status, physical details, and parent device.

- **Charts**. Displays the following metrics over the time period, if available:

- **Data Rate**. Plots values for Data Rate, Data Read Rate, and Data Write Rate.
- **Ops Rate**. Plots values for Ops Rate, Read Ops Rate, and Write Ops Rate.

- **Latency.** Plots values for latency.

- **% Busy.**

Ops Rate (block I/O)
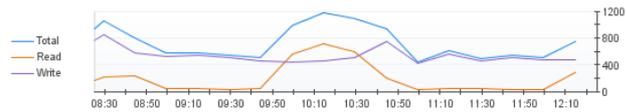
- **Alarm Summary**. Displays alarms on the controller.

3   Review Port performance in the **Port** tab.

- **FC Ports/IP Ports charts**.

   □ If the operational link speeds for the ports are available, a chart will be displayed that shows the performance of the ports based on their average utilization in the time period.

   □ If the operational link speeds for the ports are not available, a chart will be displayed with the top three ports with the highest average Data Rate in the time period.

- **Port Details**. List the ports, their status and physical state, and current values for Data Rate and Ops Rate. Click a 〰 Sparkline to plot metric values over the time period.

ℹ | **NOTE:** Port metrics are not available for NetApp filers. The Ports tab is not displayed.
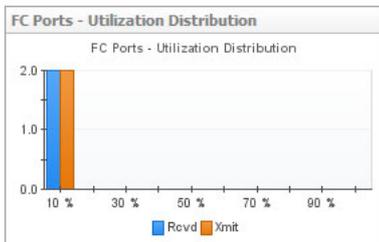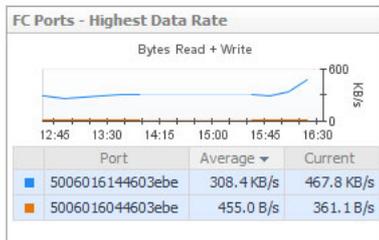
4   To investigate further:

- Click a port name. See Investigating an Array/Filer Port.
- Click an alarm. See Assessing Storage Alarms.

Investigating a Directory

In Isilon storage arrays, directories are mounted by datastores. The data displayed in the dashboard reflects values for the directory over the selected time range. The Directory dashboard has one tab.

To explore a directory:

1   On a dashboard, click a directory name.

   The Directory dashboard opens.

2   Review overall performance in the **Summary** tab.

▪ **Details**. Displays the directory's status, physical details, and parent device.

▪ **Topology**. Displays the connections from datastores to the selected directory.

3   To investigate further, click an icon to see more detail about the entity it represents, and if desired, select a component name in the detailed view to navigate to the dashboard for that component.

Investigating an EqualLogic Member

The data displayed in the dashboard reflects values for the selected EqualLogic array member over the time range. This walkthrough describes the contents of each of the tabs.

To explore an EqualLogic member:

1   In a topology diagram or from the EqualLogic Storage Array dashboard, click an array member name.

The Member Node dashboard opens.

2   Review overall performance in the **Summary** tab.

▪ **Related Inventory.** Displays a list of components from the perspective of the member (rather than the storage array).

▪ **Resource Utilization charts**. Compares resources used by the member against resources used by the pool.

- **Capacity Summary charts**. Displays Used Capacity and Available Usable Capacity.
- **Data Rate charts**. Plots values for Data Read Rate and Data Write Rate.
- **Ops Rate charts**. Plots values for Read Ops Rate and Write Ops Rate.
- **Latency charts**. Plots values for Read Latency and Write Latency.

- **Member Network Load**. Plots the member's Send Util and Rcv Util over the time period.

- **Summary and Resource Information**. Displays physical details about the member.

- **Alarm Summary**. Displays alarms on the member.

3 Click the **Network** tab.

Displays the same information as the Network tab on the EqualLogic Storage Array dashboard, but the data reflects only the selected member. For more information, see Dell EqualLogic Storage Array.

4 Click the **Disks** tab.

Displays only the disks used by the selected member. For more information, see Common Component Disk Tab Data.

Investigating an FC Switch Port

The data displayed in the dashboard reflects values for the component over the selected time range. This walkthrough describes the contents of each of the tabs.

> **i** | **NOTE:** If the port is a Brocade logical ISL, no metrics are available.

To explore a switch port:

1 On a dashboard, click an FC switch port.

The FC Switch Port dashboard opens.

2 Review overall performance in the **Summary** tab.

- **Details**. Displays the port's status, physical details, parent switch, parent fabric, VSAN (if applicable), and current values for Data Rate, Frame Rate, Link Error Rate, and Non-Link Error Rate. Click a 〰 Sparkline to plot metric values over the time period.
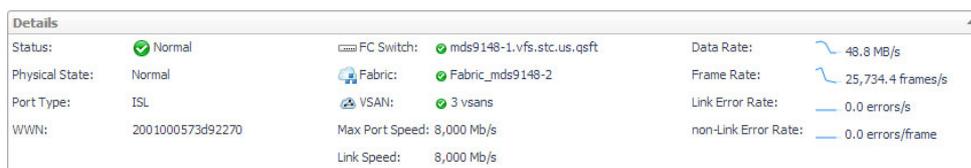
- **Charts**. Charts plot the following metric pairs over the time period:

  - **Data Rate**. Plots values for Data Receive Rate and Data Send Rate.
  - **Utilization**. Plots values for Rcvd Utilization and Xmit Utilization.
  - **Frame Rate**. Plots values for Frame Receive Rate and Frame Send Rate.
  - **Errors**. Plots values for Link Error Rate and Non-Link Error Rate.
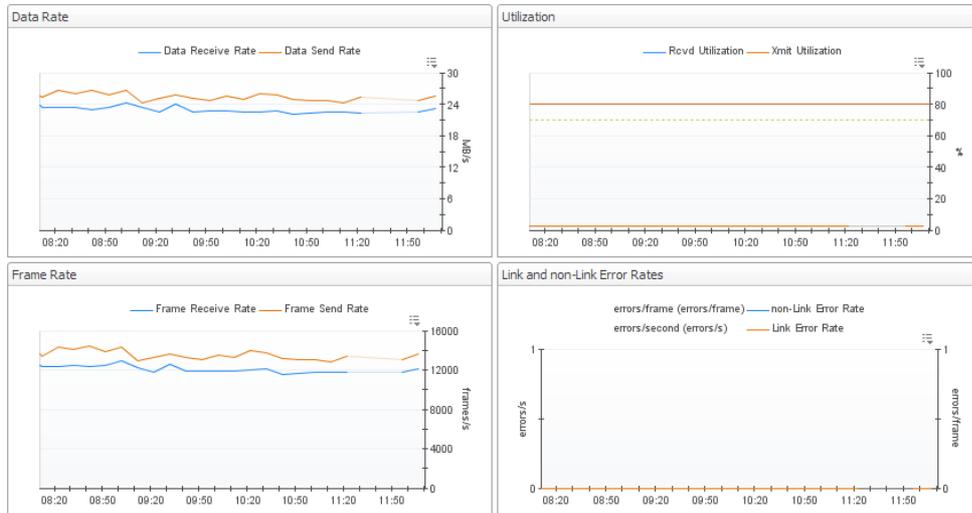
- **Alarm Summary**. Displays alarms on the port.

3   Click the **Topology** tab.

The contents of this tab depends on the type of port selected.

ISL Port:

- **Switch-to-Switch Connectivity diagram**. Displays the selected ISL port (left box) and its connection to another ISL port (right box). Click a port icon for details about the device connected to the port.
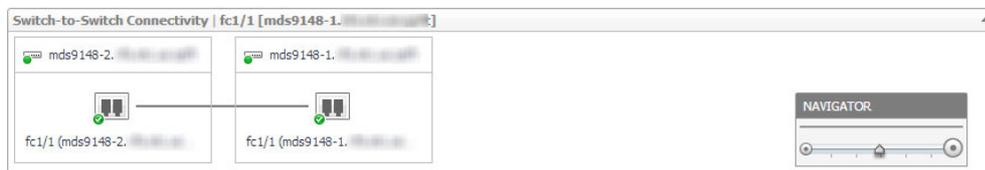
- **Topology Table (Inter-Switch Connections)**. Identifies all ISL port connections from this port's parent switch to other switches in the fabric.

N Port:

- **Basic Connectivity (table)**. Displays the ESX hosts and/or physical hosts connected to the selected N port through their host ports. An N port can have connections to multiple host ports using NPV technology.

> **i** **TIP:** If hosts in the Host Name column are *(unknown)*, you may be able to use dependency processing to infer the host names associated with the host ports. For instructions, see Inferring Physical-Host-to-Storage Relationships.

- **Basic Connectivity (diagram)**. Displays the selected N port (left box) and its connection to a filer or storage array port (right box). Click a port icon for details about the device connected to the port.

- **Select Host Port(s)**. Controls the set of hosts displayed in the Port Dependencies table.

- **Port Dependencies**. On separate tabs, displays connections to LUNs (though the selected port) from virtual machines, ESX or Hyper-V servers, and physical hosts. If the selected port has problems or failures, the connected VMs or hosts may exhibit performance problems.

4 To investigate further:

- Click a VSAN link and then select the name of the VSAN. Exploring a Cisco VSAN.

- Click an alarm. See Assessing Storage Alarms.

Investigating an Isilon Node

The data displayed in the dashboard reflects values for the selected Isilon node over the time range. This walkthrough describes the contents of each of the tabs.

***To explore an Isilon node:***

1 In a topology diagram or from the Isilon Storage Array dashboard, click a member node name.

The Member Node dashboard opens.

2 Review overall performance in the **Summary** tab.

- **Related Inventory.** Displays a list of components from the perspective of the member node (rather than the storage array).

- **IFS Capacity**. The chart displays IFS Capacity: Free and IFS Capacity Used for the IFS file system. In addition, the total capacity is broken down into hard disk drive and solid state drives metrics as follows:

  - **Total**. IFS Capacity: Total and IFS Capacity: Free
  - **HDD**. IFS Capacity: HDD Total and IFS Capacity: HDD Free
  - **SSD**. IFS Capacity: SDD Total and IFS Capacity: SDD Free

- **Node Network Load**. Charts plot the following metric pairs:

  - **External Network Throughput**. Plots the Send Data Rate and Rcv Data Rate for the external network over the time period.

ℹ **TIP:** If you prefer to see the Send Util (% of max) and Rcv Util (% of max) based on the rated maximum speeds of the ports (actual port speeds are not available from Isilon arrays) in the external network, ask your Foglight for Storage Management Administrator to edit the registry variable *StSAN_StoragePortShowUtilMax* and set `ISLN_E_IP=true`.

  - **Internal Network Throughput**. Plots values for Send Data Rate and Rcv Data Rate.
  - **Clients**. Clients connected versus clients that are actively using the network.

▪ **Node Performance**. Charts plot the following metrics for the selected node over the time period: % Busy, Latency, L1 Cache Hit Rate, L2 Cache Hit Rate, Data Read Rate, Data Write Rate, Read Ops Rate, and Write Ops Rate.
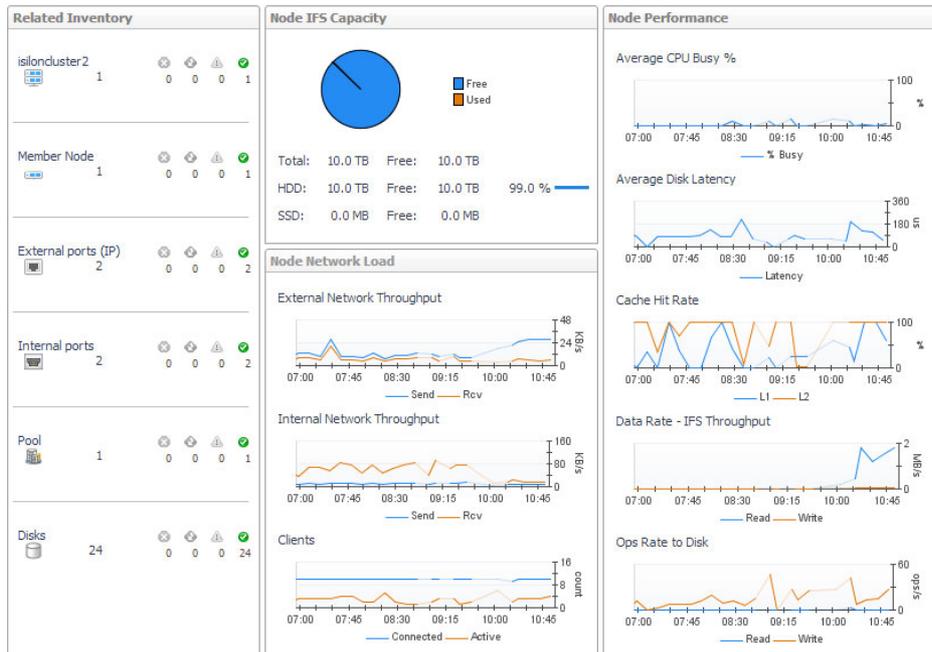
▪ **Summary and Resource Information**. Displays physical details about the member node.

▪ **Alarm Summary**. Displays alarms on the member node.

3 Click the **Network** tab.

Displays the same information as the Network tab on the Isilon Storage Array dashboard, but the data reflects only the selected member node. For more information, see EMC VPLEX Storage Array.

4 Click the **Disks** tab.

Displays disks used by the selected member. For more information, see Common Component Disk Tab Data.

Investigating a LUN

A LUN (logical unit number) represents a logical SAN block storage device on an array or filer that can be exposed for mapping to a server. The data displayed in the dashboard reflects metric values for the LUN over the selected time range. This walkthrough describes the contents of each of the tabs.

To explore a LUN:

1 On a dashboard, click a LUN name or icon.

The LUN dashboard opens.

2 Review overall performance in the **Summary** tab.

▪ **Details**. Displays the LUN's status, physical details, parent device and capacity metrics.

- **Charts**. Plot values over the time period for these metrics, if available: Ops Rate, Data Rate, Latency, % Busy, Cache Hit Rate, and Average Queue Depth.
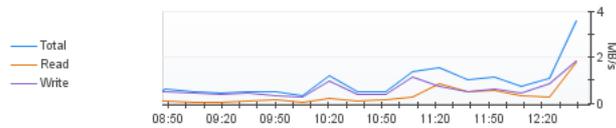
- **Pool Details**. Identifies the pools to which the LUN belongs.

    Non-clustered storage arrays — Displays performance and capacity metrics for the pools relevant to the selected LUN. For more information, see Performance Metrics and Capacity Metrics.

    EqualLogic storage arrays—Displays the same information as the Pool Details view on the Pools-Members tab of the EqualLogic Storage Array dashboard, but the data reflects only the pools relevant to the selected LUN. For more information, see Dell EqualLogic Storage Array.

- **Alarm Summary**. Displays alarms on the LUN.

3   Click the **Topology** tab.

    Displays the datastores, CSVs, or logical disks that get their physical storage from the selected LUN, the VMs that do the I/O, and if dependency processing is enabled, the (most likely) physical host connected to the LUN. For more information on dependency processing, see Inferring Physical-Host-to-Storage Relationships.
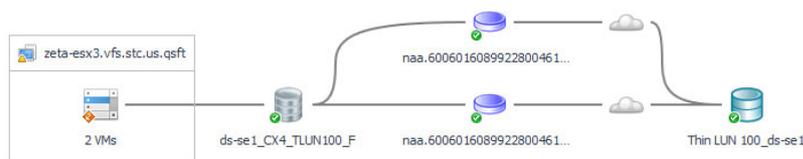
LUN providing storage to Hyper-V VMs
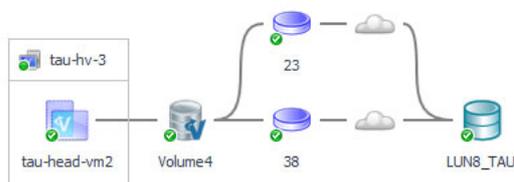
- Click a **Cloud** icon to reveal the ports and paths from disks extents to the LUN, through a particular server. For more information, see Exploring Connectivity with SAN Topology Diagrams.

- Click an icon, then select a component name to navigate to the component dashboard. For example, if you select the VM icon, you can see a list of the VMs that use the storage and select one that warrants further investigation.

4   Click the **SAN Data Paths** tab.

Displays the datastores or servers, CSVs or logical disks that get their physical storage from the selected LUN, and the VMs that do I/O to them and the LUN.

5   Review the I/O Paths table to assess the worst performing path segment of the possible data paths between each disk extent and the LUN during the time period. This helps you to identify bottlenecks resulting in high latency. For general information about how to use a Data Paths tab, see Exploring I/O Performance with SAN Data Paths. For information specific to the LUN Data Path tab, see below.

> **i** | **TIP:** For metrics that have thresholds, the color of the bars highlight data values that fall within normal, warning, critical, and fatal thresholds.Thresholds are set in the registry variables *StSAN.FCSwitchPortUtilization.*[*Warning*|*Critical*|*Fatal*].

IO Paths for LUN: LUN 107 (APM00101301407)							
ESX/VM	Latency	Data Rate	% Total I/O in ESX	ESX FC Ports -> SAN Util	SAN -> A/F Ports Util	% Total I/O at LUN	
delta-esx1.usacclab.monosphere.com	6 ms	27 KB/s					
delta-fms-vm10		27 KB/s	100 %	0 %	0 %	100 %	
delta-esx2.usacclab.monosphere.com	0 ms	0 KB/s					

> **i** | **NOTE:** The column headings may vary between VMware and Hyper-V. Where the names differ, the column headers will be listed for VMware and Hyper-V respectively.

- **ESX/VMs** or **Hyper-V Server/VM**. List of servers and the VMs they host.

- **Latency**. Average latency per operation in the time period.

- **Data Rate**. Average data rate for I/O from the ESX or VM to the LUN over the time period.

- **% Total I/O in ESX** or **% Total I/O in Hyper-V Server**. When multiple VMs on a server are performing I/O to the same LUN, displays the percentage of the total I/O performed by this VM.

- **ESX FC Ports --> SAN Util** or **Hyper-V Server FC --> Ports SAN Util**. Displays the busiest link (read or write utilization) over a time period. Click the cell to display all the port links. Review the topology diagram to see the ports and link utilization. Data is not available for IP ports.

- **SAN --> A/F Ports Util**. Displays the busiest link (read or write utilization) over the time period. Click the cell to display all the port links. Review the topology diagram to see the ports and link utilization. Data is not available for IP ports.

- **% Total I/O at LUN**. When VMs on multiple servers are doing I/O to the same LUN, displays the percentage of the total I/O performed by this server.

- **LUN Latency (ms).** Displays the latency of LUN in ms.

6   Review the diagram to understand the path from disk extents through the SAN to LUNs. The topology diagram is enhanced to show the FC ports and to display latency, link utilization, and for controllers, percent busy.

Latency   Link utilization   Percentage busy
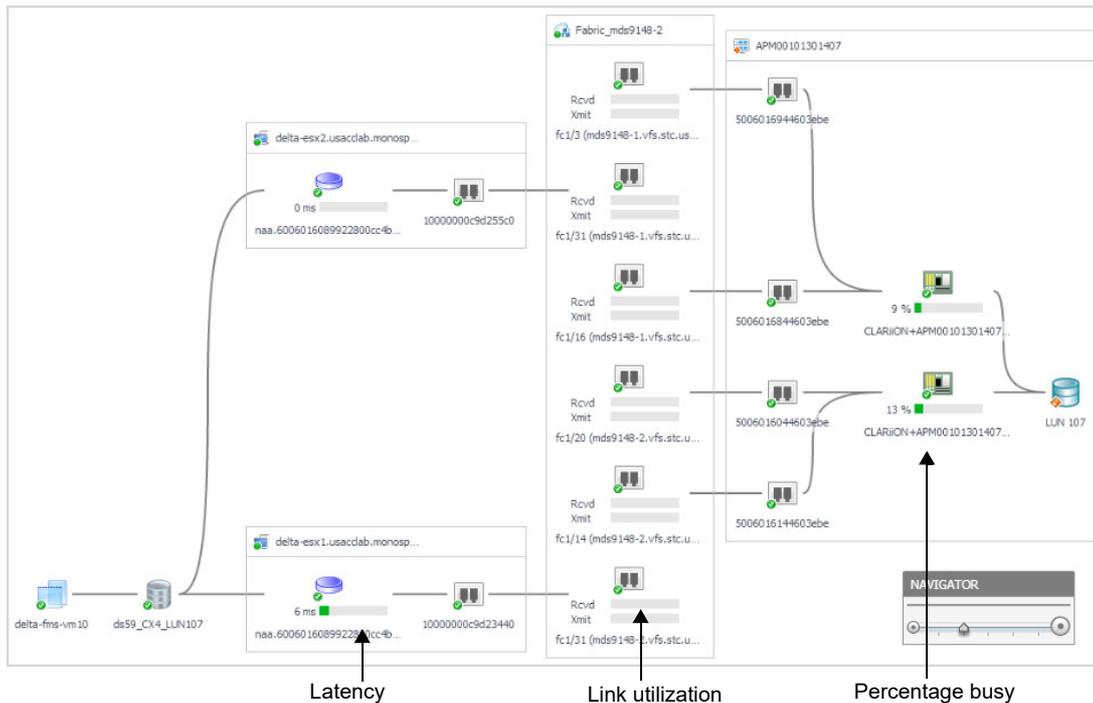
> **i** | **NOTE:** When physical hosts are inferred by dependency processing and not monitored directly by agents, the disk extents on the host that map to the selected LUN are unknown and therefore no latency values are available. For instructions on how to enable dependency processing, see *Inferring Physical-Host-to-Storage Relationships*.

7 To investigate further:

- Click a host, VM, or virtual storage name or icon. See the *Managing Virtualized Environments User and Reference Guide*.

- Click a disk name or icon. See Investigating a Physical Disk.

- Click a port name or icon. See Investigating an Array/Filer Port.

- Click a controller name or icon. See Investigating a Controller.

- Click an alarm. See Assessing Storage Alarms.

Investigating a NASVolume

A NASVolume is a volume whose physical storage is on a filer or unified storage supplier. It can be mounted by an ESX host to provide the physical storage for a datastore using NFS. The data displayed in the dashboard reflects metric values for the NASVolume over the selected time range. This walkthrough describes the contents of each of the tabs.

To explore a NASVolume:

1 On a dashboard, click a NASVolume name.

The NASVolume dashboard opens.

2 Review overall performance in the **Summary** tab.

- **Details**. Displays the volume's status, physical state, physical details, parent devices, and alarms on disks in the volume. Also displays current values for Advertised NASVolumes Size, Used Capacity, and % Used.

- **Charts**. Displays the following metrics over the time period:

  - **Data Rate**. Plots values for Data Read Rate and Data Write Rate.
  - **Ops Rate**. Plots values for Read Ops Rate, Write Ops Rate and Other Ops.
  - **Latency**. Plots values for Read Latency and Write Latency.

- **Aggregate Details**. Displays values for Total Usable Capacity, Available Usable Capacity % Available, Advertised NASVolumes Size, and Overcommitment.


- **Alarm Summary**. Displays alarms on the NASVolume.

3   Click the **Topology** tab.

Displays the datastores that get their physical storage from the selected volume as a NAS mount and the VMs that do I/O to these datastores. For more details, click an icon or an entity name. For more information about using this view, see Exploring Connectivity with SAN Topology Diagrams.
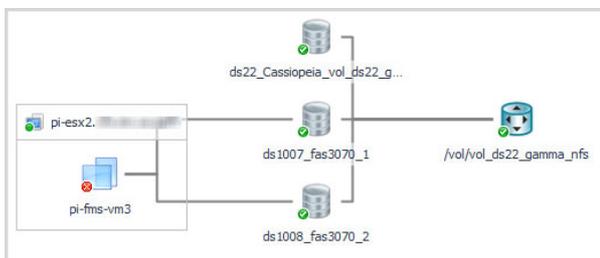
4   Click the **Disks** tab.

Displays the disks used by the NASVolume. For more information, see Common Component Disk Tab Data.

5   To investigate further:

- Click a host, VM, or datastore name or icon. See the *Managing Virtualized Environments User and Reference Guide*.

- Click an alarm. See Assessing Storage Alarms.

Investigating a Physical Disk

The data displayed in the dashboard reflects values for the selected disk over the selected time range. The Physical Disk dashboard has only one tab.

To explore a physical disk:

1   On a dashboard, click a disk name.

2   Review overall performance in the **Summary** tab.

- ▪ **Disk Details**. Displays the disk's status, physical details, parent device, and size if available.

  - □ **Physical State:** Displays the physical state the of disk. It will be marked as "**No Information**" if the disk does not commit any performance data. To mark disks as "**Removed**", click on "**No Information**" link and confirm the disk is removed physically by pressing "**Removed**" button.
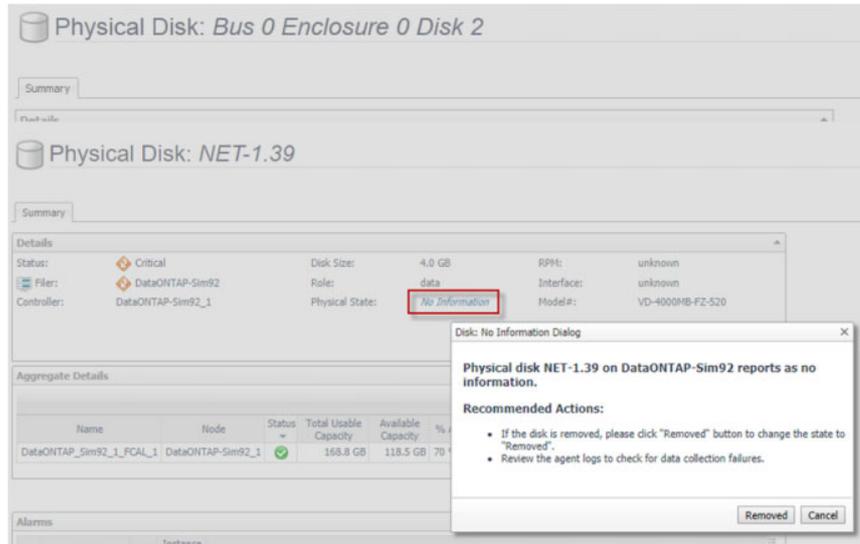
> **i** | **NOTE:** Selecting "**No Information Disks**" metric from Show Disks With drop down shows
> the disks with no metrics provided by the Agent. Selecting "**Removed Disks**" metric from
> Show Disks With drop down shows the disks manually marked as "Removed" Physical State
> in No Information Dialog.
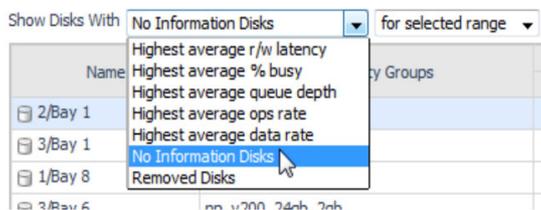
- ▪ **Charts**. Displays the following metrics over the time period:

  - **Data Rate**. Plots values for Data Rate, Data Read Rate, and Data Write Rate.
  - **Ops Rate**. Plots values for Ops Rate, Read Ops Rate, and Write Ops Rate.
  - **Latency**. Plots values for Latency, Read Latency, and Write Latency.
  - **Busy %**. Plots values for % Busy.

  - **Queue Depth.** Plots depth of the queue.
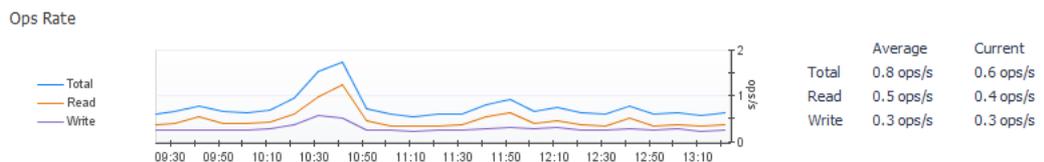
- ▪ **Pool Details (Arrays only)**. Displays performance and capacity metrics for the pools to which this disk contributes resources. For more information, see Performance Metrics and Capacity Metrics. To investigate a pool, click its name. For more information, see Investigating a Pool.

EqualLogic storage arrays—Displays the same information as the Pool Details view on the Pools-Members tab of the EqualLogic Storage Array dashboard, but the data reflects only the pools relevant to the selected disk. For more information, see Dell EqualLogic Storage Array.

Isilon storage arrays—Displays the same information as the Pool Details view on the Pools tab of the Isilon Storage Array dashboard, but the data reflects only the pools relevant to the selected disk. For more information, see EMC VPLEX Storage Array.

▪ **Aggregate Details (Filers only)**. Lists the aggregates to which this disk contributes resources. For each aggregate, displays its name, status, physical state, and current values for Total Usable Capacity, Available Usable Capacity % Available, Advertised NASVolumes Size, and Overcommitment. To investigate an aggregate, click its name. See Investigating an Aggregate.

▪ **Alarm Summary**. Displays alarms on the disk.

Investigating a Pool

Displays a summary of details for the selected pool, including a selection of size, capacity, data rate, and latency metrics. The data displayed in the dashboard reflects values for the pool over the selected time range.

The Pool dashboard is very similar for non-clustered storage arrays and EqualLogic storage arrays. The Isilon storage array requires its own Pool dashboard, which is discussed separately. The following walkthroughs describe the contents of each of the tabs.

Pool belonging to a non-clustered storage array or EqualLogic storage array

To explore a pool:

1 On a dashboard, click a pool name.

   The Pool dashboard opens.

2 Review overall performance in the **Summary** tab. From here you can initiate further analysis of the pool in terms of performance and, in some cases, pool capacity.

- **Details**. Displays the pool's status, parent storage array, physical state, health score, and current values for Total Advertised LUNs Size, Total Usable Capacity, Available Usable Capacity, Overcommitment, Total Raw Capacity, and Available Raw Capacity, if available.

- **Charts**. Displays the following sets of metrics over the time period, if available:

  - **Data Rate**. Plots values for Data Rate, Data Read Rate, and Data Write Rate.
  - **Ops Rate to Disk**. Plots values for Ops Rate, Read Ops Rate, and Write Ops Rate.
  - **Latency**. Plots values for Latency, Read Latency, and Write Latency.
  - **Average Queue Depth**. Plots values for Average Queue Depth.
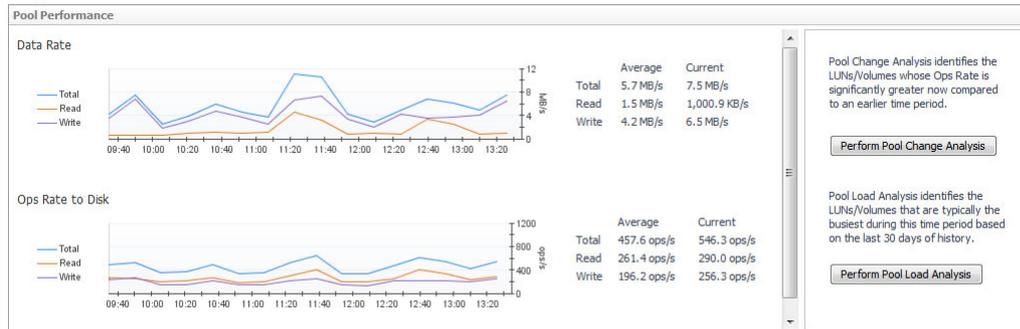
- **Perform Pool Change Analysis**. Click to identify the LUNs primarily responsible for increased I/O. For more information, see Analyzing the Pool.

- **Perform Pool Load Analysis.** Click to identify the busiest LUNs, and rank them based on their activity during the same time range *over the last 30 days*. For more information, see Analyzing the Pool.

- **Alarm Summary**. Displays alarms on the pool.

3 Click the **Capacity** tab.

- **Capacity Summary.** Pools in most arrays will display data similar to the data shown below.
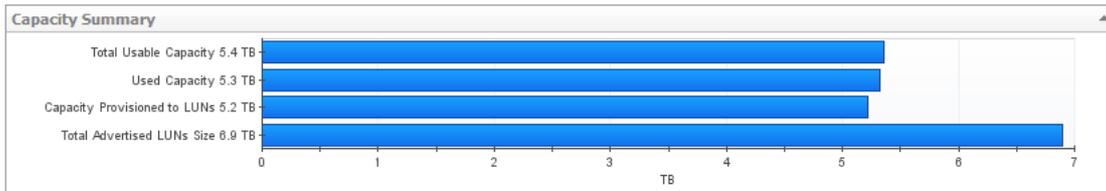
    For some arrays, pool capacity in Usable terms is not available. Then the capacity summary will display with total capacity in raw terms instead of usable terms.
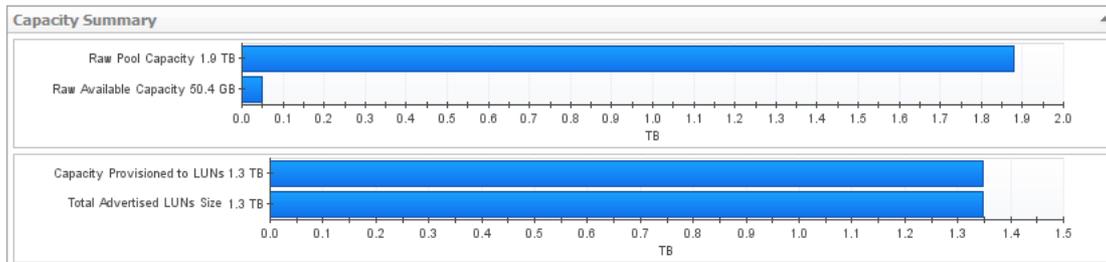
- **Capacity Usage Trends.** Provides a visual display of the estimated capacity consumption in the future, based on a regression analysis of the historical capacity consumption.

  If time until full shows n/a, it means enough historical data hasn't been collected yet to perform an analysis. Mouse over for additional information. For more information, see Capacity Trending.
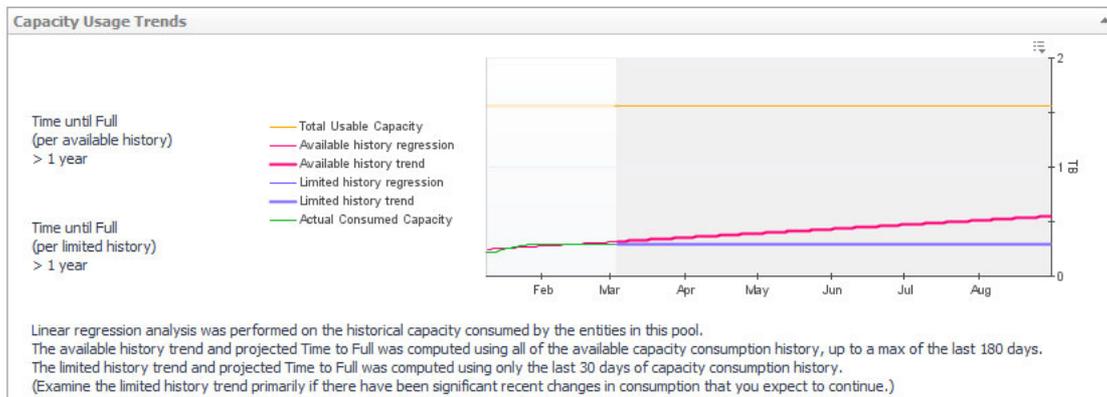
4 Click the **LUNs** tab. This tab displays the LUNs carved from this pool.

A LUN (logical unit) is the block storage element made available by an array or filer to a server.

- **Top 5 LUNs**. Displays the top five LUNs with the highest average value for Data Rate, and the performance metrics most useful for this array or filer.
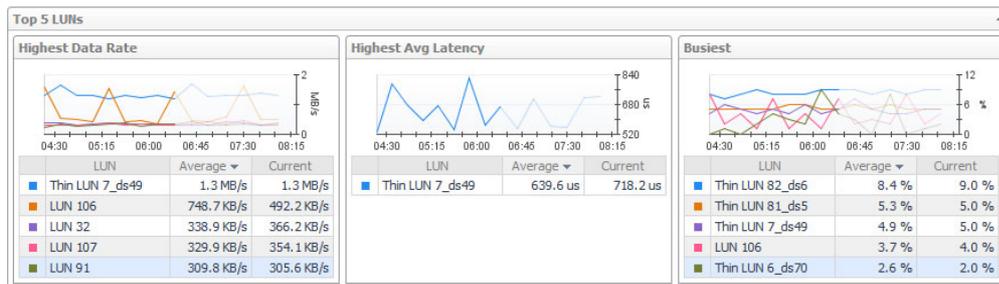
- **LUN Status Filter**. Click to show only LUNs with the selected status in the LUN Details table.

- **LUN Details**. For each LUN, displays its status, physical state, parent pool or aggregate, and whether the LUN is used by an entity in the monitored environment. The metric columns display current values for Data Rate, Ops Rate, Latency, % Busy, Average Queue Depth, L1 Cache Hit Rate, and Total Advertised LUNs Size. Click a 〰 Sparkline to plot metric values over the time period.

  ℹ | **NOTE:** If a metric is not available for this particular array or filer, the column is not displayed.

  The remaining columns provide the following details:
  - **Protection**. Displays the type of protection in use on the LUN, such as the RAID level.
  - **Thin**?. Indicates whether the LUN is thin-provisioned (true) or thick-provisioned.

  - **IQN**. Displays the iSCSI Qualified Name. Click the **Customizer** ▤ to add this column.
  - **vFiler**. *Filers only*. Displays the name of the virtual filer associated with the LUN.

- **Alarm Summary**. Displays alarms on LUNs.

5 Click the **Disks** tab.

Displays the disks used by the selected pool. For more information, see Common Component Disk Tab Data.

6 To investigate further:

- Click a LUN name. See Investigating a LUN.

- Click a disk name. See Investigating a Physical Disk.

Pool belonging to an Isilon storage array

To explore a pool for an Isilon storage array:

1   On an Isilon-related dashboard, click a pool name.

The Pool dashboard opens.

2   Review overall performance in the **Summary** tab.

- **Pool Details**. Displays the pool's status, parent storage array, and current values for IFS Capacity: Free and IFS Capacity Used for the IFS file system. In addition, the total capacity is broken down into hard disk drive and solid state drives metrics as follows:

  - **Total**. IFS Capacity: Total and IFS Capacity: Free
  - **HDD**. IFS Capacity: HDD Total and IFS Capacity: HDD Free
  - **SSD**. IFS Capacity: SDD Total and IFS Capacity: SDD Free
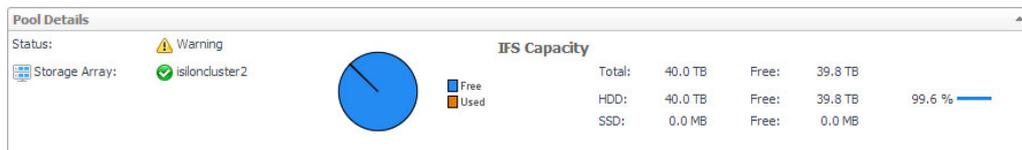
- **Performance**. Charts plot the following metrics for the selected pool over the time period: % Busy, Latency, L1 Cache Hit Rate, L2 Cache Hit Rate, Data Read Rate, Data Write Rate, Read Ops Rate, and Write Ops Rate.

- **Node Status Filter**. Click to show only member nodes with the selected status in the Node Details table.

- **Node Details**. For each node belonging to the pool, displays its name, status, physical state, and current values for Data Rate, % Busy, Latency, L2 Cache Hit Rate, IFS Capacity, and IFS Capacity: Free. Also displays the worst status of the node's disks, external network ports, and internal network ports, and identifies the node's parent pool. Click a Sparkline to plot metric values over the time period.

You can add the following metrics to the table by clicking the **Customizer** ≡ icon: L1 Cache Hit Rate, Send Data Rate and Rcv Data Rate. You can also choose to display other Isilon details, such as Total Disk IOPS and Model.

- **Alarm Summary**. Displays alarms on the pool.

3   Click the **Capacity** tab.

- **Capacity Usage Trends.** Provides a visual display of the estimated capacity consumption in the future, based on a regression analysis of the historical capacity consumption.

  If time until full shows n/a, it means enough historical data hasn't been collected yet to perform an analysis. Mouse over for additional information. For additional information, see Capacity Trending.
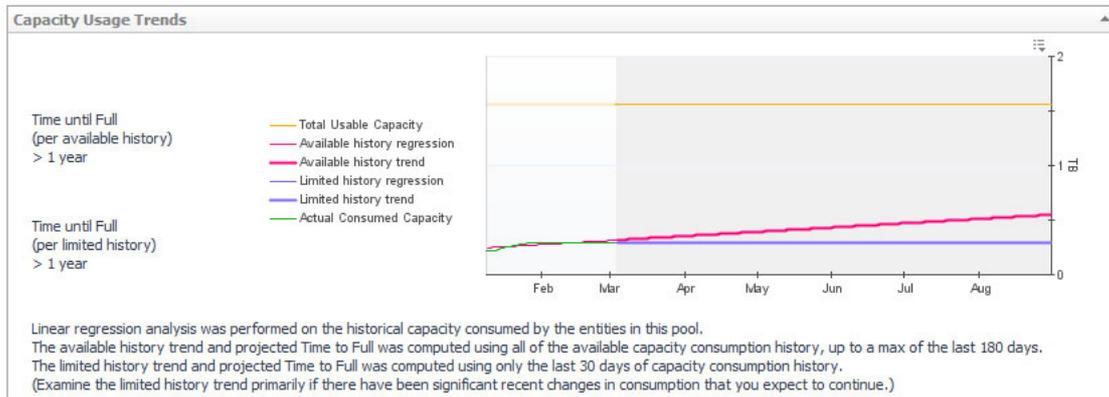
4   Click the **Network** tab. Assess the performance of the ports in the External Network from the perspective of the pool.

- **Charts**. Plot aggregated values for Send Data Rate and Rcv Data Rate, and Packet Errors % for the external network connections over the time period.

- **Port Status Filter**. Click to show only ports with a selected status in the Port Details table.

- **Port Details**. For each port used by the external network, identifies the port name, parent node, status, physical state, and current values for Send Data Rate, Rcv Data Rate, and Packet Errors %.

  Also displays the maximum speed of the port. Click a 〰 Sparkline to plot metric values over the time period.

  > **i** | **NOTE:** When the registry variable *StSAN_StoragePortShowUtilMax* is set to show port utilization, the chart and table display Rcv Util (% of max) and Send Util (% of max).
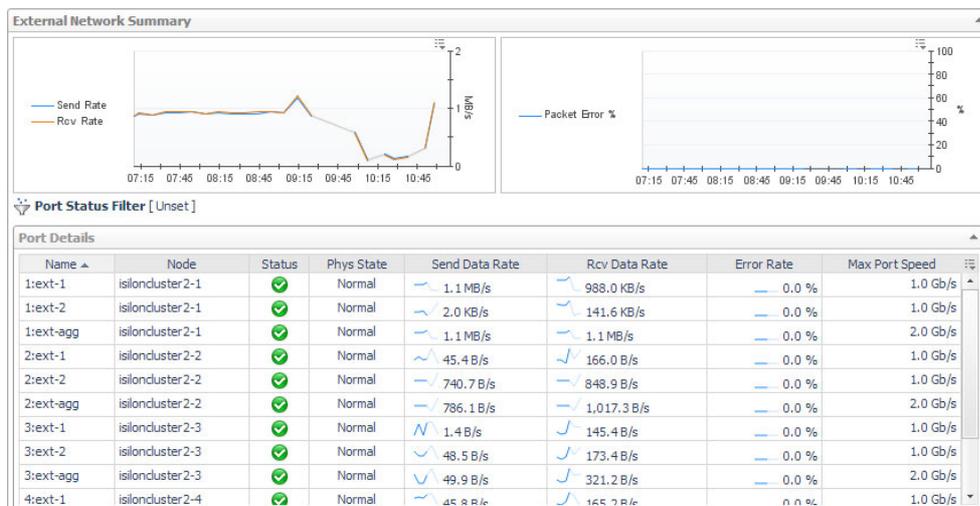
- **Alarm Summary**. Displays alarms on ports used by the external network.

5   Click the **Disks** tab. Displays the disks used by the selected pool. For more information, see Common Component Disk Tab Data.

6   To investigate further, click a disk name. See Investigating a Physical Disk.

Common Component Disk Tab Data

The Disks tab can be found on the following dashboards:

- Member/Node

- Pool

- Aggregate

- NASVolume.

The Disks tab displays the physical disks associated with the selected entity.

> **i** | **NOTE:** The images in this section reflect an EMC CLARiiON storage array, but the views should be similar for any filer or storage array. For filers, where the word *pool* is used, it means *aggregate*.

- **Top 5 Disks**. Displays the top five disks with the highest average value for Ops Rate and the performance metrics most useful for this array or filer.
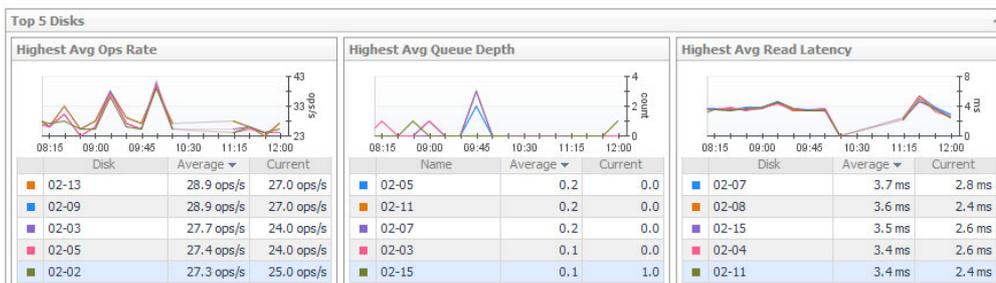
- **Disk Status Filter**. Click to show only disks with the selected status in the Disk Details table.

- **Disk Details**. For each disk, identifies its status, physical state, parent pool or aggregate, and Disk Size, and then displays current values for Ops Rate, % Busy, Average Queue Depth, Data Rate, and Latency. Click a ⌇ Sparkline to plot metric values over the time period.

    > **i** | **NOTE:** If a metric is not available for this particular array or filer, the column is not displayed.

    The remaining columns provide the following details:
    - **Role**. Displays the role played by the disk in the pool, such as disk or spare.
    - **RPM**. Displays revolutions per minute as reported by the vendor.
    - **Disk Interface**. When available, displays the type of interface, such as SATA or SCSI.
    - **Member**. *EqualLogic and Isilon only*. Displays the name of the member node where the disk physically resides.

Disk Status Filter [Unset]

Name	Status	Phy State	Pools	Disk Size	Ops Rate	Avg Q Depth	Data Rate	Latency	Role
01-01	✓	Normal	Assigned	465.8 GB	0.0 ops/s	0.0	0.0 B/s	0.0 ms	Disk
01-05	✓	Normal	Assigned	465.8 GB	0.0 ops/s	0.0	0.0 B/s	0.0 ms	Disk
01-09	✓	Normal	Assigned	465.8 GB	0.0 ops/s	0.0	0.0 B/s	0.0 ms	Disk
01-13	✓	Normal	Assigned	465.8 GB	0.0 ops/s	0.0	0.0 B/s	0.0 ms	Disk
01-14	✓	Normal	Assigned	465.8 GB	0.0 ops/s	0.0	0.0 B/s	0.0 ms	Disk
01-16	✓	Normal	Assigned	465.8 GB	0.0 ops/s	0.0	5.0 KB/s	0.0 ms	Disk
02-01	✓	Normal	Assigned	558.9 GB	0.0 ops/s	0.0	0.0 B/s	0.0 ms	Spare
02-02	✓	Normal	Assigned	558.9 GB	25.0 ops/s	0.0	376.0 K...	3.6 ms	Disk
02-03	✓	Normal	Assigned	558.9 GB	24.0 ops/s	0.0	357.0 K...	3.6 ms	Disk
02-04	✓	Normal	Assigned	558.9 GB	24.0 ops/s	0.0	422.0 K...	3.7 ms	Disk
02-05	✓	Normal	Assigned	558.9 GB	24.0 ops/s	0.0	344.0 K...	3.6 ms	Disk

• **Alarm Summary**. Displays alarms on disks.

Investigating VPLEX Storage

To gain a complete picture of the performance of a VPLEX storage device, you need to understand how its child components are performing.

This section covers the following topics:

- Introducing VPLEX Virtualization Components Dashboards
- Investigating Director - Ports
- Investigating a Virtual Volume
- Investigating a Storage Volume

Introducing VPLEX Virtualization Components Dashboards

The VPLEX Virtualization Components dashboard is a drill-down view that displays virtualization details about a selected VPLEX storage array, performance and capacity metrics, and alarms.

For information about each type of VPLEX Virtualization Components dashboard, see the following topics:

- Investigating Director - Ports
- Investigating a Virtual Volume
- Investigating a Storage Volume

Investigating Director - Ports

The data displayed in the dashboard reflects values for the VPLEX storage over the selected time range. This walkthrough describes the contents of each of the tabs.

To explore a director:

1   On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2   In the **Storage Explorer** dashboard, click the director name in the **Director** table.

3   In the **Summary** tab, review performance in terms of key metrics.

- **Details**. Displays physical details about the selected director.
- **Charts**. Plot values over the time period for these metrics, if available: Ops Rate, Data Rate, % Busy, Frontend Abort, and Average Queue Depth.
- **Alarm Summary**. Displays alarms on the selected director. To investigate further, click an alarm. See Assessing Storage Alarms.

4   In the **Ports** tab, Shows the history performance data of the port, including Ops Rate, Data Rate, and Latency.

To explore a port:

1   On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2   In the **Storage Explorer** dashboard, click the director name in the **Port** table.

3   In the **Summary** tab, review performance in terms of key metrics.

   - **Details**. Displays physical details about the selected port.

   - **Charts**. Plot values over the time period for these metrics, if available: Ops Total, Bytes Read, Bytes Write, Read Latency, and Write Latency.

   - **Alarm Summary**. Displays alarms on the selected port. To investigate further, click an alarm. See Assessing Storage Alarms.

Investigating a Virtual Volume

A Virtual Volume represents a logical SAN block storage device on an VPLEX array that can be exposed for mapping to a server. The data displayed in the dashboard reflects metric values for the Virtual Volume over the selected time range. This walkthrough describes the contents of each of the tabs.

To explore a Virtual Volume:

1   On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2   In the **Storage Explorer** dashboard, click the Virtual Volume in the **Virtual Volumes Detail** table.

3   In the **Summary** tab, review performance in terms of key metrics.

   - **Details**. Displays the Virtual Volumes's status, physical details, parent device and capacity metrics.

   - **Ops Chart**. Shows the history Ops Rate of the virtual volume.

   - **Data Rate Chart**. Shows the history Data Rate of the virtual volume.

   - **Latency Chart**. Shows the history Latency of the virtual volume.**Alarm Summary**. Displays alarms on the VPLEX array.

   - **Alarm Summary**. Displays alarms on the selected virtual volume. To investigate further, click an alarm. See Assessing Storage Alarms.

4   In the **Frontend Topology** tab, displays the dependency mapping from virtual machines to the virtual volume. Click a cloud node to display the network dependency mapping from VM disks to the virtual volume.

5   In the **Backend Topology** tab, displays the dependency mapping from the virtual volume to the destination LUNs. Click a cloud node to display the network dependency mapping from the virtual volume to the destination LUNs.
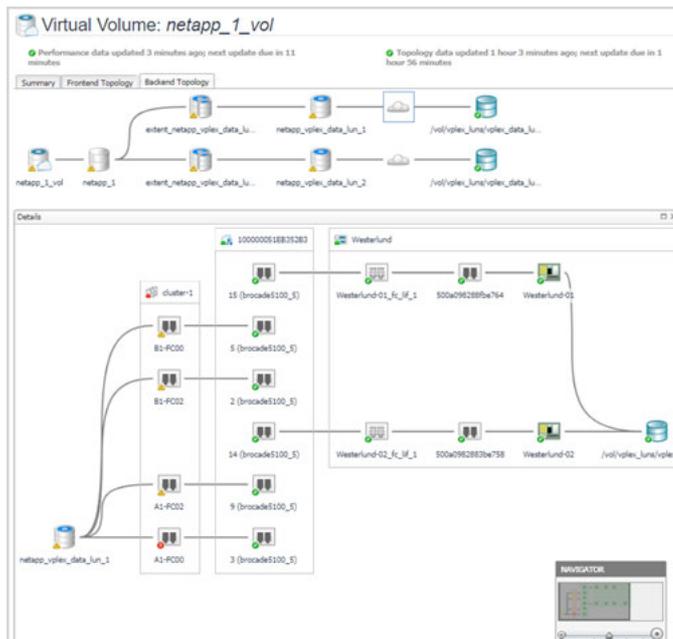
Investigating a Storage Volume

The data displayed in the dashboard reflects values for the selected storage volume over the selected time range. The Storage Volume dashboard has only one tab.

To explore a storage volume:

1   On the navigation panel, under Dashboards, click **Storage & SAN > Storage Explorer**.

2   In the **Storage Explorer** dashboard, click the Storage Volume in the **Storage Volumes Detail** table.

3   In the **Summary** tab, review performance in terms of key metrics.

- **Details.** Displays the storage volume's status, physical details, parent device, and size if available.

- **Charts**. Plots values for Data Rate, Data Read Rate, and Data Write Rate.

- **Alarm Summary**. Displays alarms on the selected storage volume. To investigate further, click an alarm. See Assessing Storage Alarms.

4   In the **Topology** tab, displays the dependency mapping from virtual volumes to the storage volume, and the dependency mapping from the storage volume to destination LUNs. Click a cloud node to display the network dependency mapping from the storage volume to destination LUNs.

Troubleshooting Storage Performance

Administrators may receive problem reports from stakeholders about the performance of a VMware virtual machine (VM). When the suspected cause is storage, the Administrator can run an automated analysis using the Storage Troubleshooting dashboard. The analysis can quickly rule out a storage issue, allowing the Administrator to focus on other areas. Conversely, if a storage issue is found to be contributing to poor performance, the results of the analysis clearly highlights the datastores or RDM disk extents that require attention.

This section is intended for Foglight for Storage Management users with the role of Storage Administrator. It describes how to start an investigation, analyze the results, and change latency thresholds. It also summarizes the algorithm used to identify and assess storage performance issues.

This section describes the following topics:

- Starting a Troubleshooting Investigation
- Analyzing Storage Issues
- Analyzing the Pool
- Changing Latency Thresholds
- Understanding the Troubleshooting Algorithm

Starting a Troubleshooting Investigation

Before beginning an investigation, you should ask the person reporting the issue the following questions:

- What is the host name of the affected virtual machine?
- When did you first notice the performance issues? The reported time frame determines how you set the zonar time range.

To investigate a potential storage performance issue:

1 On the navigation panel, under Dashboards, click the **Insights** tab, and then click **Live Troubleshooter**.

2 Set the zonar to encompass the reported time frame, up to a maximum of 8 hours.

   The zonar is located in the upper right corner of the dashboard.
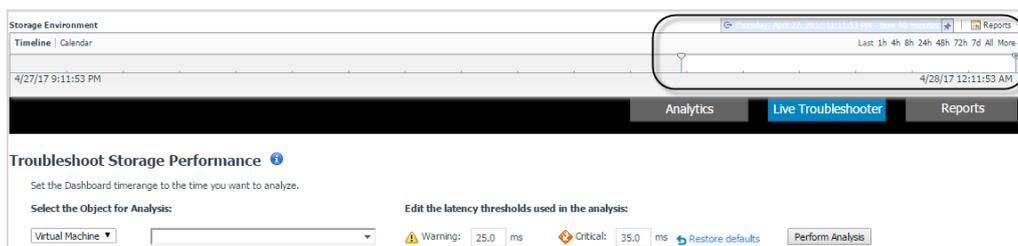
3   Type the host name of the virtual machine.

4   The latency threshold values are set automatically based on the latency registry variables. If different
    values would be more meaningful for your analysis, see Changing Latency Thresholds.

5   Click **Perform Analysis**.

    Depending on the complexity of the analysis request, it may take a little time before the results of the
    analysis appear on the dashboard.
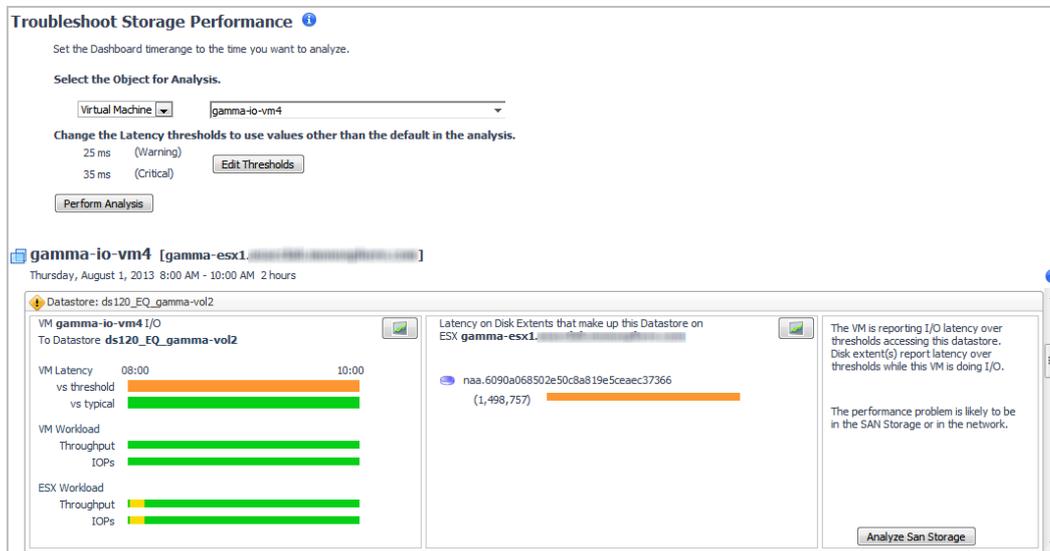
    Recall that a virtual machine can get its storage either from a datastore (connected in turn to one or more
    disk extents or to a NASVolume) or directly from an RDM disk extent (without a datastore). In the analysis
    results, each datastore or RDM disk extent that is connected directly to the selected virtual machine is
    represented by a separate view.

6   Review the icons displayed in the title bars of each datastore/RDM view.

    ▪   If a **Normal** ✅ icon appears in *all* title bars, the performance issue is *not* storage-related. This
        investigation is complete.

    ℹ   **TIP:** In some cases, the Diagnosis summary (right-hand panel) may contain hints about where to look
        next. For example, increased I/O (as compared to typical I/O for this period) may indicate that an
        application is behaving differently than before.

    ▪   If the **Attention** ⚠ icon appears in one or more title bars, continue your investigation following the
        workflow described in Analyzing Storage Issues.

Analyzing Storage Issues

If the view for a datastore or RDM disk extent shows the **Attention** ⚠ icon, the troubleshooting algorithm has
discovered evidence of a performance problem related to storage. The problem may or may not be in the SAN
Storage environment. Review the details to determine the cause of the performance issue.

Each datastore/RDM view has three summary panels (from left to right):

•   VM I/O to Datastore/RDM (first panel)

•   Latency for Disk Extents (middle panel)

•   Diagnosis (last panel)

A virtual machine may be connected to multiple datastores and RDM disk extents, each of which may report varying degrees of problems. When a virtual machine has more than one datastore/RDM view, start by scanning the timeline bars in the **VM I/O to Datastore/RDM** panel to identify a datastore/RDM with consistently slow I/O performance or significant changes from typical performance.

The following workflow describes one way to identify a latency problem in the collected SAN Storage environment. While the details in your investigation may differ, the general workflow should be similar to this one.

To analyze storage issues:

1   In a view showing the **Attention** ⚠ icon, scan the **VM I/O to Datastore/RDM** summary (first panel). Look for timeline bars that primarily show colors such as yellow, orange, or pink, that is, any color other than green (which represents acceptable activity).
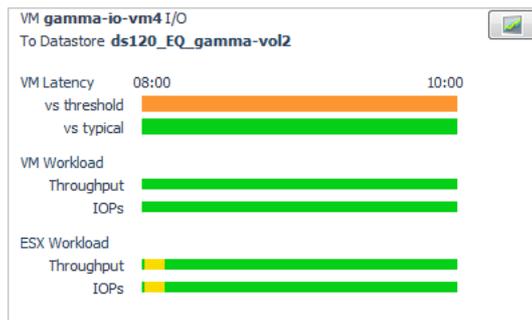
In this example, the VM Latency vs Threshold timeline is orange, which means the virtual machine is consistently exceeding the default latency thresholds that were specified for the analysis. We should focus our investigation here.

The VM Latency vs Typical timeline is green, which means that the latency is typical for the time period; this behavior has been going on for some time. The typical values are statistical values determined by IntelliProfile from activity within the last 30 days.

2   Now look at the **Latency for Disk Extents** summary (middle panel) to identify the disk extents that are contributing to the problem.

> **i** | **NOTE:** When a datastore is connected to a NASVolume, this panel is empty.
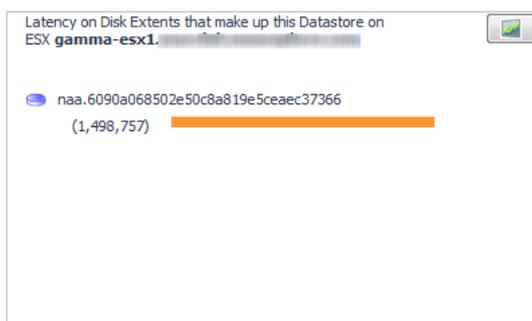
In this case, there is only one disk extent attached to the datastore. Its timeline is orange, which means the disk extent is exceeding latency thresholds. The number in brackets indicates that the virtual machine was performing I/O to the disk extent while the VM was experiencing latency. The larger the number, the more I/O was occurring. When this number is zero, no I/O occurred while the VM was experiencing latency.

> **i** | **TIP:** In your own investigations, you may have more than one disk extent, in which case you may be able to see that one disk extent is slow while the others are normal. Or you may have multiple virtual machines sharing the same disk extent. In this case, the Diagnosis panel may display a message to let you know that the latency may not reflect this virtual machine alone.

3   Next, review the notes in the Diagnosis summary (last panel).

The VM is reporting I/O latency over thresholds accessing this datastore. Disk extent(s) report latency over thresholds while this VM is doing I/O.

The performance problem is likely to be in the SAN Storage or in the network.

Analyze San Storage
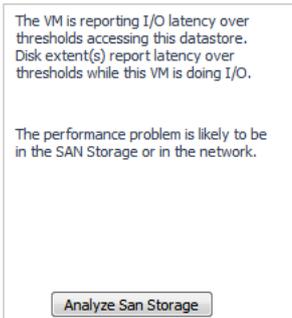
In this case, one of the notes describes a correlation between the virtual machine latency and the disk extent latency. The other note points toward a problem in the SAN Storage or the network, and below is a button that begins an analysis of the SAN Storage.

> **i** | **NOTE:** If the troubleshooting algorithm determines that the issue is likely in the SAN Storage environment, and if the SAN Storage is provided by an element that the Foglight for Storage Management system is monitoring, the Analyze SAN Storage button appears in the Diagnosis panel.

4   Before analyzing the SAN Storage, you may want to quantify the performance issue by reviewing the metric values that underlie the timeline bars in the summary panels.

   a   In the **VM I/O to Datastore/RDM** summary, click the **Chart** icon.
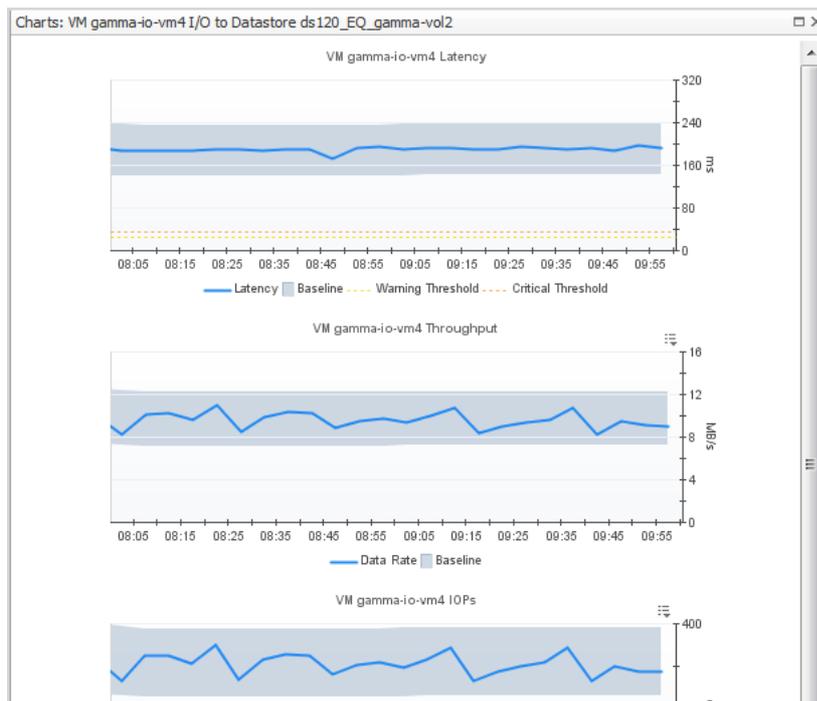
The charts show the values of the metrics over the time period. Some charts also contain a baseline range, which shows a statistical range of values encountered over the last 30 days. Spikes outside of the normal range represent a significant change in behavior that may warrant further investigation.

In this case, the top chart shows that the VM I/O latency is hovering around 200 m/s, well above the default 25 m/s and 35 m/s latency thresholds.

   b   Close the window.

   c   In the **Latency for Disk Extents** summary, click the **Chart** icon.

Charts: Latency on Disk Extents that make up Datastore ds120_EQ_gamma-vol2
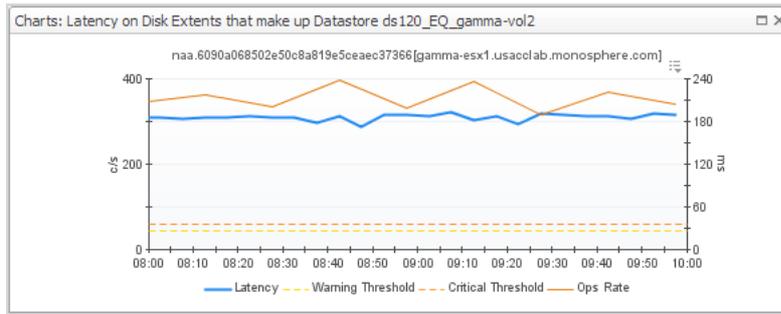
The chart shows the disk extent latency values hovering around 180 m/s. The latency here may reflect the activity of multiple VMs doing I/O or the performance within the ESX itself. It is clear that a significant delay is occurring in the disk extent.

    d   Close the window.

5   In the Diagnosis panel, click **Analyze SAN Storage**.

The Storage-Side Analysis window breaks down performance by the Extent, the LUN to which it belongs, and the pool to which the LUN belongs.
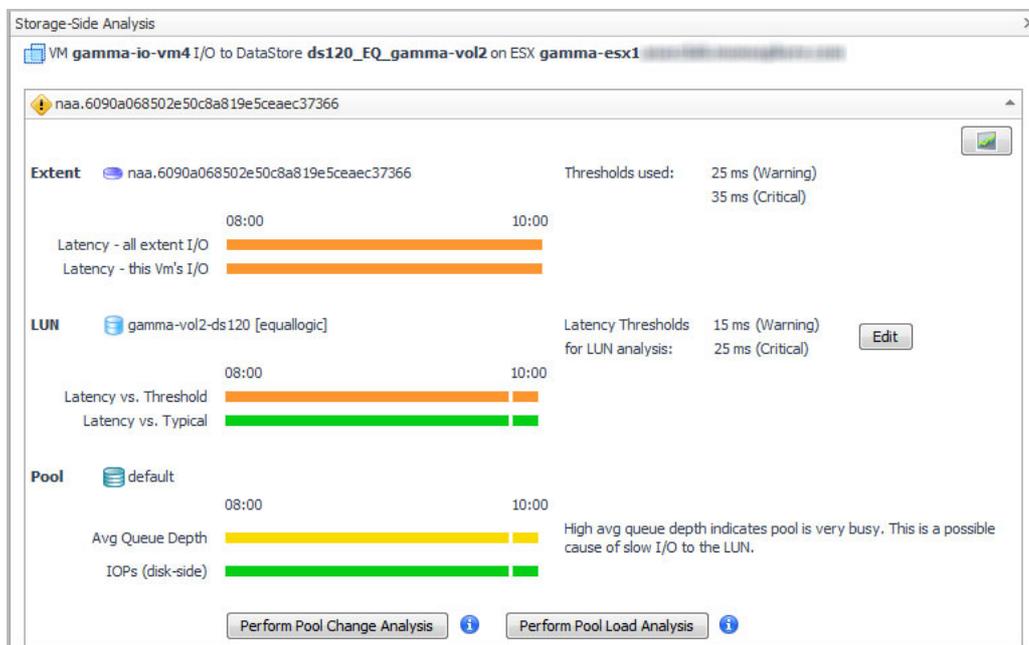
This view shows that the disk extent is slow for all virtual machines and for the selected virtual machine. The disk extent to LUN I/O performance also exceeds latency thresholds, though its current performance is within the baseline range, which shows a statistical range of typical values encountered over the last 30 days. This indicates the high latency has been occurring for some time. If you want to see the metric

values, click the **Chart** icon.

6   The next step in the investigation depends on the state of the pool.

    ▪   If the pool timeline bars are green, the investigation is complete.

    ▪   If the pool timeline bars are a color other than green, you can analyze the changes within the pool and the load on the pool. Continue the investigation by following the workflow in Analyzing the Pool.

In this example, the pool's Avg Queue Depth timeline bar is yellow. The note beside the bar suggests that this may be a cause of slow I/O to the LUN. The pool warrants further investigation.

Analyzing the Pool

When pool timeline bars show abnormal average queue depth or ops rate, analyze the changes within the pool and the load on the pool.

- **Perform Pool Change Analysis**. The Pool Change analyzer identifies the LUNs primarily responsible for increased I/O. It compares LUN activity in the problem time range with LUN activity during the same time range in the past. Changes are reported in terms of average operations rate and change amount.

- **Perform Pool Load Analysis**. The Pool Load analyzer identifies the busiest LUNs and ranks them based on their activity during the same time range over the last 30 days (not the current time frame). Activity is measured in operations per second.

To analyze the pool:

1 From the Server-Side Analysis window or the Pool Explorer window, click **Perform Pool Change Analysis**.
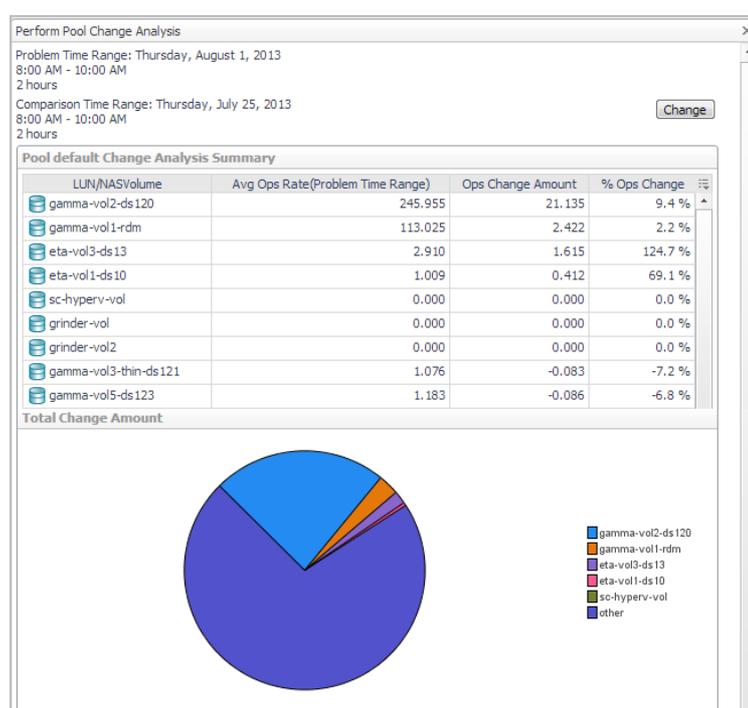
The analyzer compares activity for all the LUNs in the pool during the problem time range with their activity a week ago. In this example, the table and pie chart confirm that the LUN with the highest average operations rate and change amount is the LUN that includes the disk extent used by the poor performing virtual machine.

> **i** | **TIP:** You can change the comparison time range by clicking **Change** and selecting a new date and time range.

2 Close the window.

3 Click **Perform Pool Load Analysis**.
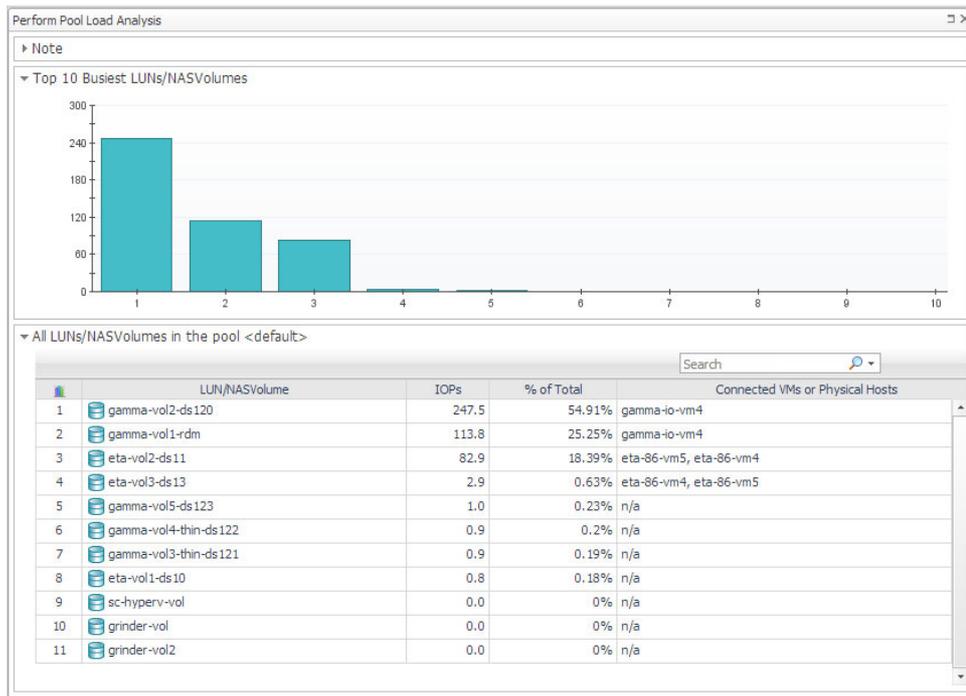
The chart and table show the top ten busiest LUNs. The analysis is based on the last 30 days of activity during this time range. In this example, the table confirms that the top two busiest LUNs are connected to the poor performing virtual machine.

4   Close the window.

The investigation is complete.

Changing Latency Thresholds

One way Foglight for Storage Management determines if the performance problem is occurring in the SAN storage environment is to evaluate latency against the thresholds defined for latency in registry variables. The latency thresholds used for analysis are, by default, the same thresholds as are used for generating latency alarms. If you think it would be helpful to adjust the threshold values for your analysis, you can change the threshold values using the Storage Troubleshooting dashboard. The original registry variables are not updated.

i | **TIP:** If you change thresholds, you can restore the default values later using the Reset button.

To change the latency thresholds:

1   In the Storage Troubleshooting dashboard, click **Edit Thresholds**.

2   Specify the new thresholds in milliseconds for one or both of **Warning** and **Critical**.

3   Click **Apply**.

Understanding the Troubleshooting Algorithm

To determine if the problem is likely to be a storage performance problem, Foglight for Storage Management evaluates latency metrics against thresholds and typical performance, and disk extent metrics against the I/O

being performed to the extent by the virtual machine. If the likely cause of the problem is slow performance in the SAN Storage environment, Foglight for Storage Management examines the LUN or NASVolume. If no circumstances, such as a rebuild, are identified as a cause of high latency, the pool is examined.

Managing Data Collection, Rules, and Alarms

ℹ **NOTE:** This section is intended for users with the role *Storage Administrator*. Some tasks also require the Foglight for Storage Management role of *Administrator* (as noted) to manage agents and rules.

You can collect additional types of relationship data, change collection schedules, manage rules, and manage alarms.

- Collecting Virtual Storage-to-SAN Relationships
- Inferring Physical-Host-to-Storage Relationships
- Modifying Data Collection Schedules (*Administrator* role required)
- Managing Foglight for Storage Management Rules (*Administrator* role required)
- Managing Alarm Settings
- Troubleshooting Database Limits

If you are looking for information about configuring Foglight for Storage Management agents and agent masters, reviewing agent alarms, creating support bundles, or backing up data, see the *Foglight for Storage Management Installation Guide*.

Collecting Virtual Storage-to-SAN Relationships

To include virtual storage-to-SAN relationships in your topology diagrams, you need to enable storage collection on your VMware or Hyper-V Performance agent. If you did not enable this option when defining the agent, you can enable it by editing the agent.

ℹ **NOTE:** If you cannot see the Administration dashboards, ask your Foglight for Storage Management Administrator to add the role *VMware Administrator* or *Hyper-V Administrator* to your user account.

To update an existing virtualization agent to add the collection of storage data:

1 On the navigation panel, under Dashboards, click **VMware > VMware Agent Administration** or **Hyper-V > Hyper-V Agent Administration**.

2 In the Agents table, locate the Agent. In the Data Collection column, you can see whether general data collection is enabled for this agent. Storage data collection, however, is not enabled by default.

3   To enable storage data collection for an agent, click the agent's **Edit** 📝 icon.

4   Select the **Enable Storage Collection** check box and click **Save**.

Inferring Physical-Host-to-Storage Relationships

If you want to understand how storage resources are being accessed by the physical hosts in your network, without using agents to monitor the hosts directly, you can enable dependency processing. Dependency processing collects FC switch zone information and LUN connection information from arrays and filers, analyzes each host port used for storage I/O, and infers the (most likely) physical host associated with the port. When dependency processing is enabled, relevant topology diagram are enhanced to show inferred hosts connected to the ports that are used for storage I/O. Connections from inferred hosts are shown as orange or blue lines.

Figure 19. SAN Topology tab
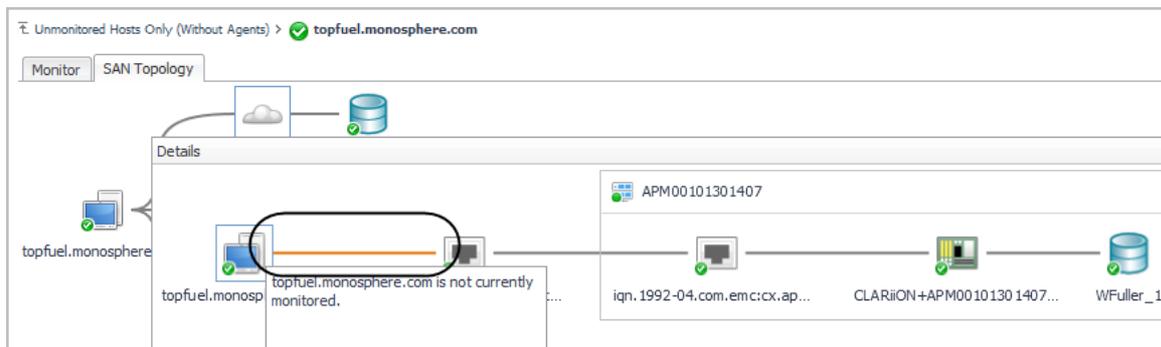
In future, if you decide you want to collect data about inferred physical hosts, you can begin monitoring the hosts by configuring Infrastructure agents. For instructions, see Reviewing Inferred Hosts.

Enabling Dependency Processing

Dependency processing requires that you have VMware Performance agents configured to monitor your vCenters, and that storage collection is enabled on the agents. For more information, see "Configuring VMware Performance Agents" in the Foglight for Storage Management Installation Guide.

To enable dependency processing:

1   On the navigation panel, under Dashboards, click **Storage & SAN** > **Storage Environment**.

2   Click the **Administration** tab.

3   Click **Enable Physical Host to Storage Dependency Processing**.

4   In the Physical Host Support message box, click **Yes**.

The dependency processing algorithm collects information and runs a host-resolution process. This may take some time.

When the processing completes, the Enable Physical Host to Storage Dependency Processing Task changes to Disable Physical Host to Storage Dependency Processing Task, and a new task, Review Physical Host FQDNs, appears in the task list.
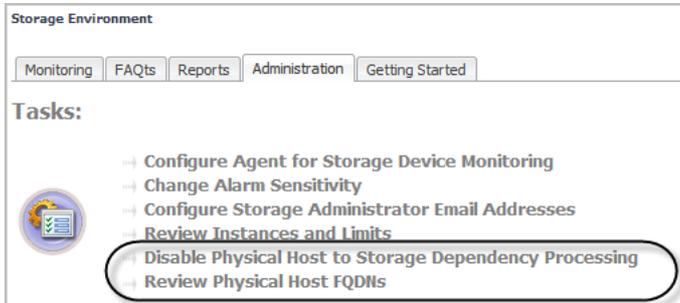
5   **Next Step**: Reviewing and Editing Host-Port Assignments

Reviewing and Editing Host-Port Assignments

After enabling dependency processing, it is a good idea to review the list of inferred hosts derived from this process. You can verify that the inferred hosts are correct for the specified port, fix errors, and provide missing host names. For this task, you use the Review Physical Host FQDNs dashboard.

> **i** | **NOTE:** The Review Physical Host FQDNs dashboard also contains host-port assignment for physical hosts that are being monitored by an agent.

To review the list of hosted identified by dependency processing:

1   On the Storage Environment dashboard, in the **Administration** tab, click **Review Physical Host FQDNs**.

The Review Physical Host FQDNs dashboard opens. The table displays the list of hosts, the associated port carrying storage I/O, zone information for switch ports, and the number and type of storage resources accessed. You can filter the contents of the table using the Show Host Ports check boxes.
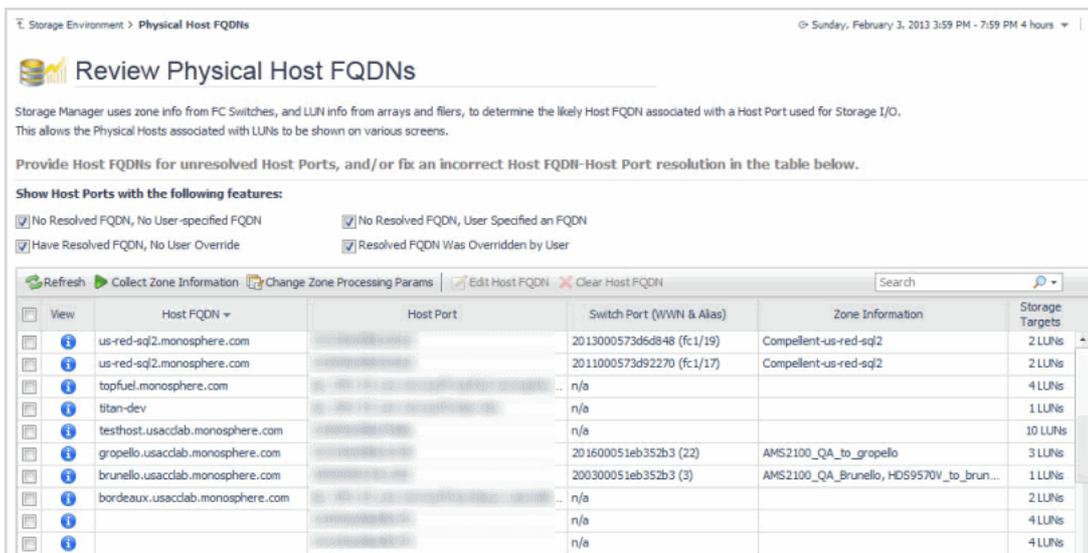
2   To add missing host names or change existing host names:

a   Click the row check boxes for the port assignments you want to change. All selected ports will be assigned the same host name.

b   Click **Edit Host FQDN**.
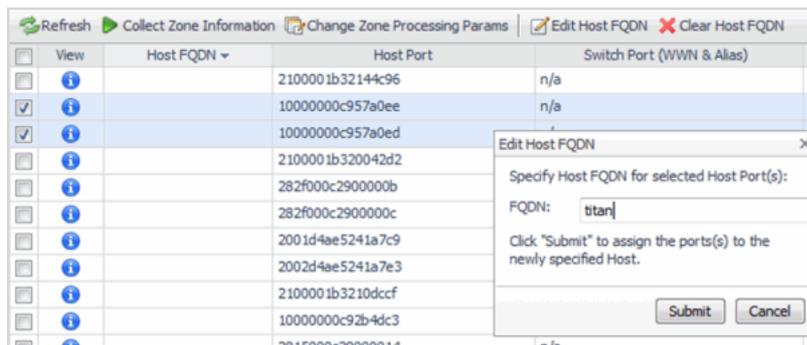
c   Type the fully qualified domain name for the host, and click **Submit**.

The table displays the new host-port assignments.

3   To remove host assignments from ports, select the row check boxes for the ports and click **Clear Host FQDN**.

▪   Clearing a user-resolved host makes the agent-resolved host active, if one exists.

▪   Clearing an agent-resolved host adds the host FQDN to a list so that it does not get reassigned to the port in the future.

Running Dependency Processing Manually

If your environment has changed, you can update inferred-host-to-storage connections immediately rather than waiting for a scheduled processing.

ℹ | **NOTE:** Edited host-port assignments are not affected by these actions.

On the Review Physical Host FQDNs dashboard, use one of the following options:

•   **Refresh**—Runs the host-resolution analysis to identify inferred hosts for ports handling storage I/O.

•   **Collect Zone Information**—Dependency processing automatically collects zone information on a nightly basis. If your environment has changed, use this button to collect updated zone information for FC switches in your environment and run the host-resolution analysis. The collection and analysis can take between five to ten minutes, possibly longer depending on the complexity of the environment.

Customizing Helper Strings for Dependency Processing

Zone names are set by the Storage Administrator and typically include the names of devices connected to ports. The dependency processing algorithm processes the zone name strings using various helper strings to identify the possible host names associated with a port. A DNS lookup is performed on the possible names to identify the most likely host FQDN. You can customize the helper stringers for your environment and improve the accuracy of the inferred hosts.

To customize helper strings for dependency processing:

1   On the Storage Environment dashboard, in the **Administration** tab, click **Review Physical Host FQDNs**.

2   Click **Change Zone Processing Params**.

The Edit Parameters for Zone Info Processing dialog box opens.

3   To specify IP addresses to ignore during dependency processing, click **Invalid IPs**. Click **Add**, specify an IP address, and click **Add**.

Some DNS setups *always* return a default IP address when a DNS lookup of a possible host name fails. If a DNS lookup of a host name returns an IP address listed in the Invalid IP table, the host name is considered invalid for dependency processing purposes.
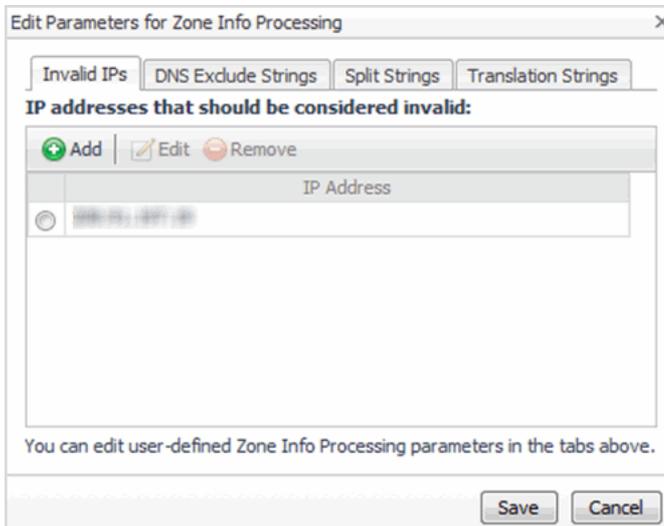
4   To specify strings that may be included in the zone information, but are known not to be host names, click **DNS Exclude Strings**. Click **Add**, specify a string, and click **Add**.
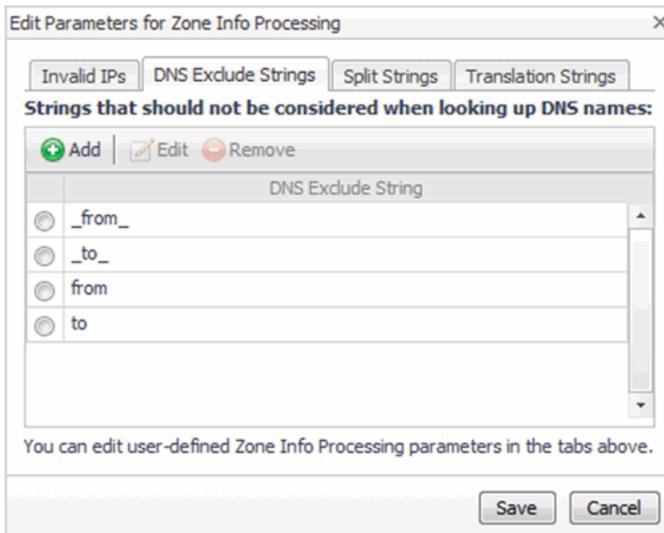
5   To specify strings used as separators for readability in the zone names, click **Split Strings**. Click **Add**, specify a string, and click **Add**.

6   To specify strings that you want to convert to other strings before performing a host name DNS lookup, click **Translation Strings**. Click **Add**, specify a string found in the zone information and the new string to use, and click **Add**.

7   When you are finished customizing parameters on all tabs, click **Save**.

Dependency processing begins. Zone information is collected using the changed parameters and host-resolution analysis is performed.

Reviewing Inferred Hosts

You can see a list of inferred hosts on the Infrastructure dashboard. From this dashboard, you can explore hosts and change their host port assignments if necessary. If you are interested in monitoring and collecting detailed data about an inferred host, you can set up an agent to monitor the host. This action moves the host from the inferred list to the appropriate monitored host list.

For more information about the Infrastructure dashboard, see the *Managing the Infrastructure Cartridge* section of the Foglight for Storage Management online help.

To review inferred hosts:

1 On the navigation panel, under Dashboards, click **Infrastructure**.

2 In the Select a Service list, select **All Hosts**.

3 In the Monitoring tab, click the **Inferred** tile.

4 In the quick view, click a host in the Inferred list and then click **Explore**.

5 Click the **SAN Topology** tab.

The SAN Topology tab displays the connections to the LUNs identified through dependency processing.
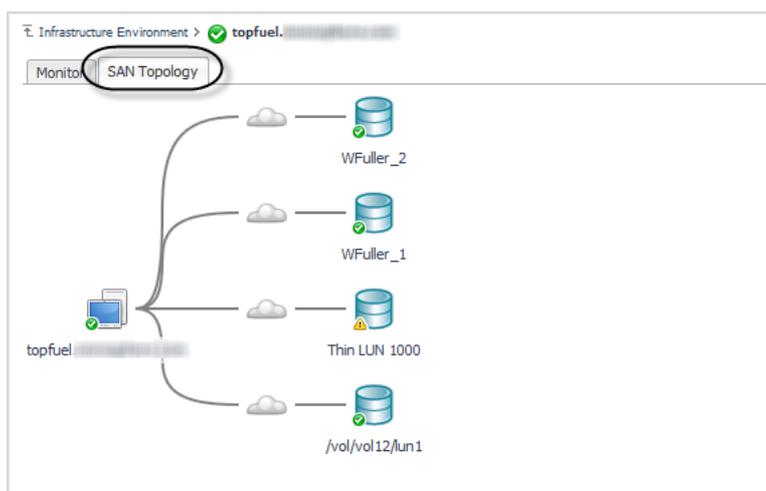
6 Click a **Cloud** ☁ icon to show the connections through a port in a Details window.

An orange line connecting a host to a port indicates that the host is an inferred host.
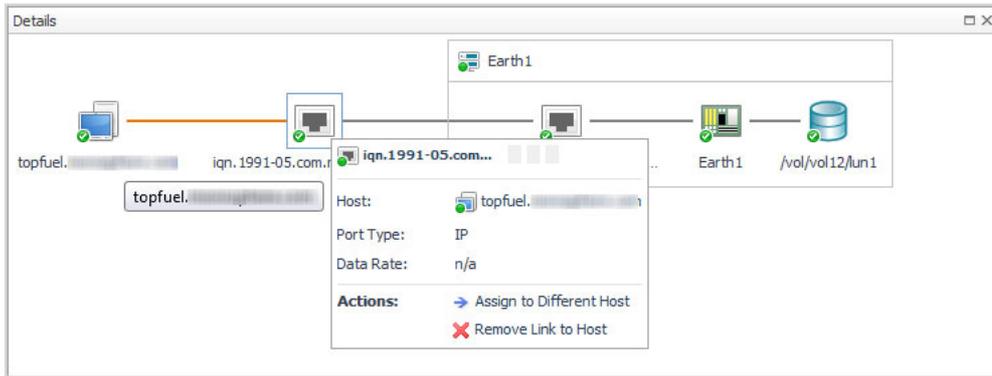
7   If the assigned host is incorrect, click the **Host Port** [icon] icon and select the desired action, such as **Assign to Different Host** or **Remove Link to Host**.

8   Close the Details window.

9   If you want to set up an agent to monitor this host, click the **Monitor** tab.

> **i** | **NOTE:** If your user credentials do not include the role *Administrator*, you need to ask someone with this role to create an agent to monitor the host.

10 Click **Configure Host Monitoring**.

11 In the Add Monitored Host wizard, follow the online instructions to add the host.

For help with the wizard, see "Adding a Monitored Host" in the *Managing the Infrastructure Cartridge* section of the Foglight for Storage Management online help.

Modifying Data Collection Schedules

Generally speaking, the default data collection schedules are suitable for most environments. If you notice that some agents take an extended time to collect topology data or performance data, and modifying your monitoring environment is not a suitable solution, you may want to change the data collection schedules for the affected agents. You can find the current duration of collections in the Edit Agent Properties dialog box.

Understanding Data Collection Types and Schedules

Storage Collector agents perform two types of collections: topology collections and performance collections.

Topology collections

During topology collections, Foglight for Storage Management gathers basic information regarding each object and its child objects. For example, on an array object, LUN, disk, and children information is gathered. Foglight for Storage Management gathers various attributes and parameters (for example, size or capacity) as well as relationship data. This relationship data is the key to understanding the basic topology and interconnects, or paths, between objects (parent to parent, child to parent and, where appropriate, child to child). Without this relationship information performance analysis would not be possible.

Performance collections

During performance collections, Foglight for Storage Management gathers the following basic types of information:

- Performance metrics for each known object (an object is known if it has previously been collected during a topology collection).

- The performance collection enumerates objects and their children. This enumeration determines if there is any change in the topology (for example, a LUN has been created, a new ESX server has been added to a cluster, or a new VM has been created). As the collector recognizes changes in the environment (sometimes in conjunction with the server) it schedules topology collections to ensure that Foglight for Storage Management continually has an accurate understanding of the underlying topology. Not all topology changes can be detected by the performance collection. A scheduled topology collection will pick up any undetected changes.

Default data collection schedules

Storage Collector agents have a default schedule for topology and performance collections, as described in the following table.

Table 20. Default data collection schedules.

Type	Collection Interval	Notes
Topology collection	3 hours	*n/a*
Performance Collection for EMC SMI-S and Hitachi AMS only	15 minutes	Defines the collection interval for an agent that monitors a storage device using SMI-S or Hitachi AMS. The management hosts from which the Storage Collector agent collects performance data using SMI-S obtain performance data from the arrays every 15 minutes. Setting the agent to collect data more frequently is inefficient, because the same data is re-collected and discarded.
Performance Collection for all others	10 minutes	Defines the collection interval for an agent that uses a different method (than those listed above) to monitor a storage device.

For information about the technologies used by Storage Collector agents to monitor the different kinds of storage devices, see "Configuring Agents to Monitor Storage Devices" in the Foglight for Storage Management Installation Guide.

Modifying Data Collection Schedules for Storage Collector Agents

> **ℹ️ NOTE:** You require the Foglight for Storage Management role *Administrator* to perform tasks that affect agents.

The collection interval can be increased to reduce the collection frequency impact in busy environments. It is not recommended to reduce the performance collection interval to less than five minutes. You can change the schedule for all agents by editing the default schedule, or clone the default schedule to create and select a specific schedule for a Storage Collector agent.

To modify storage collection schedules:

1 On the navigation panel, under Dashboards, click **Administration > Agents**.

2 Click **Agent Status**.

The Agent Status dashboard opens.

3 Select the agent whose schedule you want to change from the Agent Status view. You can select any Storage Collector agent if you are changing the default schedule.

4 Click **Edit > Edit Properties**.

The Agent Status view displays.

5 Select **Modify the properties for this agent only.**

6 Scroll down to the Data Collection Scheduler section.
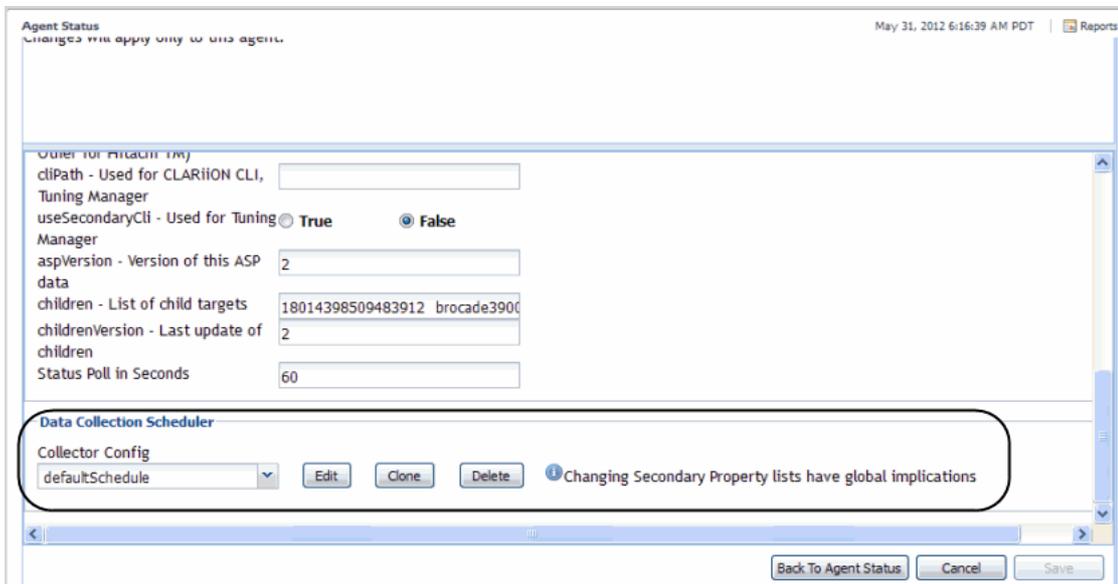
From here you can perform the following agent editing tasks:

▪ To edit an existing schedule, continue with this procedure.

▪ To create a unique schedule for an agent using clone, see Creating a unique schedule for an agent.

▪ Assign a cloned schedule to another agent, see Assigning a Cloned Schedule to Another Agent.

7 From the Data Collection Scheduler drop-down, select the schedule you want to edit.
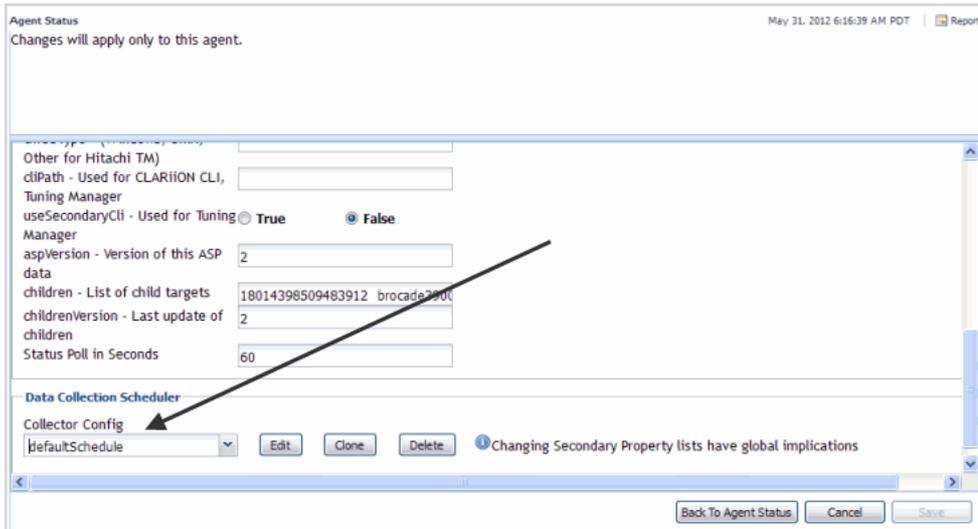
8   Click **Edit**.

The Storage Collector-*<scheduleName>* dialog box opens.

9   Click inside the field you want to edit and make the required changes.
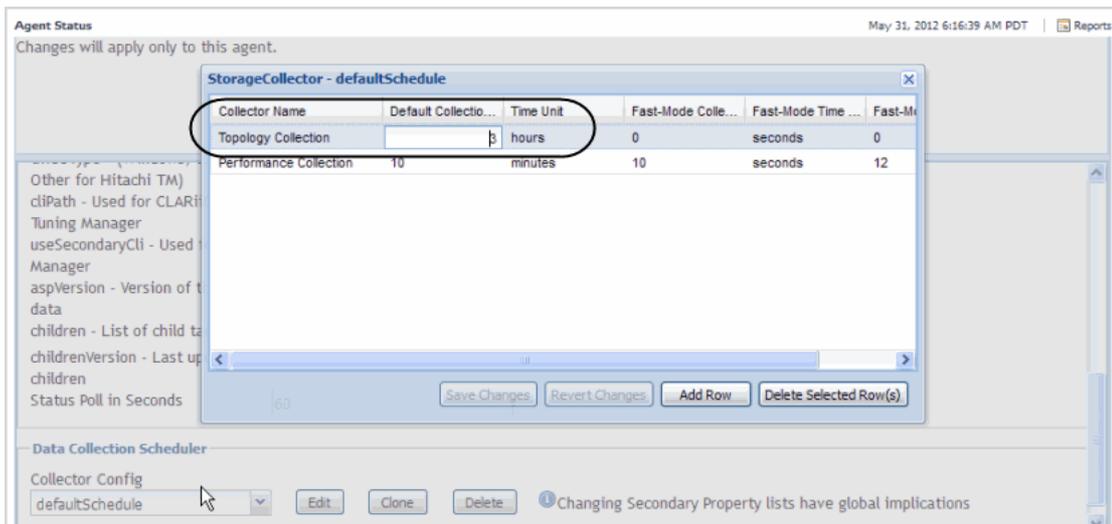
10 Click **Save Changes**.

11 Close the Storage Collector-*defaultSchedule* dialog box.

12 Click **Back to Agent Status**.

The edit is complete.

Creating a unique schedule for an agent

This procedure provides the steps required to create a unique schedule for a Storage Collector agent.

To create a unique schedule for an agent:

1   From the Agent Status view, click **Modify the private properties for this agent**.
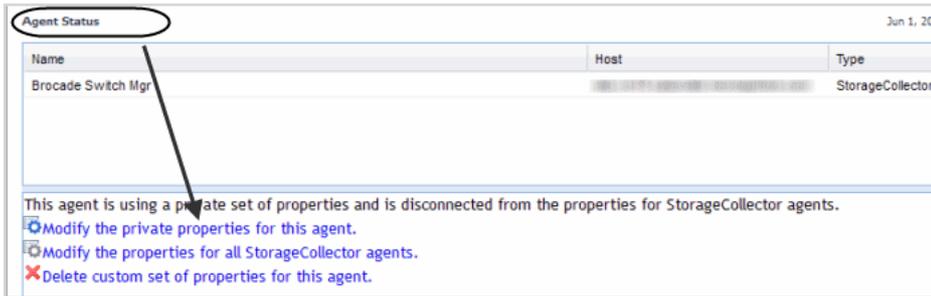
2 Scroll down to the Data Collection Scheduler section.

3 In the Data Collection Schedule section, click **Clone**.
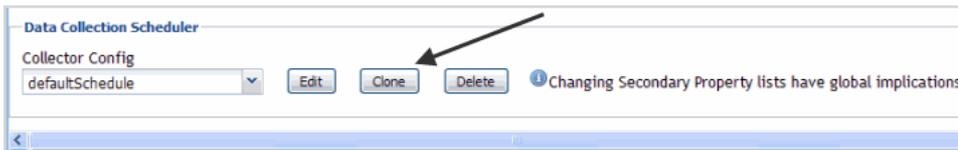
The Clone defaultSchedule dialog box opens.

4 Enter a schedule name, and click **OK**.

The newly-cloned schedule appears in the Collector Config schedule selector.

5 Click **Edit**.

The Storage Collector edit dialog box opens.

6 Click inside the field(s) to be edited.

7 Click **Save Changes** to update the new schedule.

8 Close the Storage Collector-<*name*> dialog box.

9 Click **Save** to assign the new schedule to the agent.

10 Click **Back to Agent Status**.

The edit is complete.

Assigning a Cloned Schedule to Another Agent

This procedure provides the steps required to clone a schedule to another Storage Collector agent.

To assign a cloned schedule to another agent:

1 From the Agent Status view, click **Modify the private properties for this agent**.

2 Scroll down to the Data Collection Scheduler section.

3 Click the **Collector Config** drop-down list.

4 Select the schedule you want to assign to this agent.
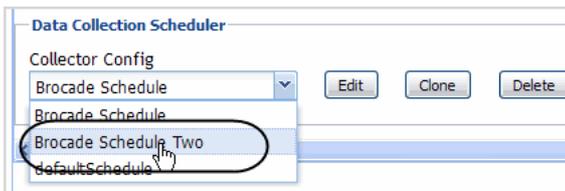
5 Click **Save** to assign this new schedule to this agent.

6 Click **Back to Agent Status**.

The edit is complete.

Managing Foglight for Storage Management Rules

> **i** | **NOTE:** You require the Foglight for Storage Management role *Administrator* to perform tasks that affect rules.

To see the list of Foglight for Storage Management rules, navigate to **Administration > Rules & Notifications > Rule Management**, and select **StorageUI** from the Cartridge list. For help with rules, open the online help from this dashboard.

All Foglight for Storage Management rule names start with *StSAN* and are organized into categories:

- **Essential**—*StSAN E*—Essential rules alert on latency issues, capacity issues, device failures, and errors.
- **Normal**—*StSAN N*—Normal rules alert on things like data traffic spikes.
- **Tuning**—*StSAN T*—Tuning rules are additional rules for situations that do not cause performance issues in most environment.

The Essential and Normal categories are enabled by default. The rules within each category can be enabled or disabled individually. By default, all rules in the Essential category are enabled, and all rules in the Normal category are disabled. You may want to review the Normal rules and enable the ones that suit your environment. Finally, you can control whether alarms are generated for rules in all categories or only some categories. For more information, see Changing Alarm Sensitivity.

You can and should modify rule conditions to better suit your storage environment. To change conditions, copy the rule and modify it. Then you can enable the new rule and disable the original rule. This approach allows you to refer back to the original rule if necessary, and also protects you from changes to the default rules that may occur during regular software updates. For more information, search for "Copying or deleting rules" in the online help.

For rules that reference registry variables for threshold values, you should modify the threshold in the registry variable, rather than modifying the rule. For help finding and editing registry variables, search for "Registry Variable" in the online help.

> **i** | **NOTE:** Rules that begin with *StSANCar* are rules used internally by the Storage cartridge, and do not generate alarms. Do not disable or alter these rules.

Managing Alarm Settings

You can control which type of rule generates alarms and also set up email notifications.

Changing Alarm Sensitivity

You can control which categories of StSAN rules generate alarms.

To set the alarm sensitivity:

1   On the navigation panel, under Dashboards, click **Storage & SAN** > **Storage Environment**.

2   Click the **Administration** tab.

3   Click **Change Alarm Sensitivity**.
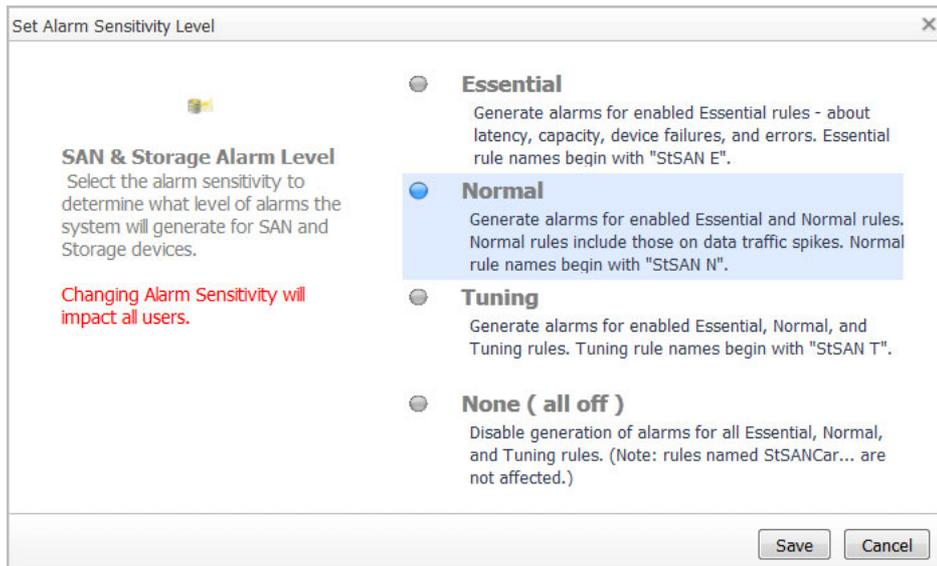
4   Select the category of rules that generate alarms or turn off alarms for all essential, normal, and tuning rules.

As noted in the option descriptions, each option includes the rule category that matches the name of the option plus the categories listed in the option above it, so selecting Tuning enables alarms for tuning, normal, and essential rules.

5   Click **Save**.

Configuring Email Notifications for Alarms

You can define a list of email addresses that receive a notification whenever an essential rule evaluates to a Critical or Fatal status. Email addresses are saved to the `StorageAdministrator` registry variable. An essential rule begins with *StSAN E* and has the email action set automatically. For more information about rules, see Managing Foglight for Storage Management Rules.

To specify email addresses:

1   On the navigation panel, under Dashboards, click **Storage & SAN** > **Storage Environment**.

2   Click the **Administration** tab.

3   Click **Configure Storage Administrator Email Addresses**.

4   Click **Add**, type an email address, and click **Add**. Repeat to add additional email addresses.
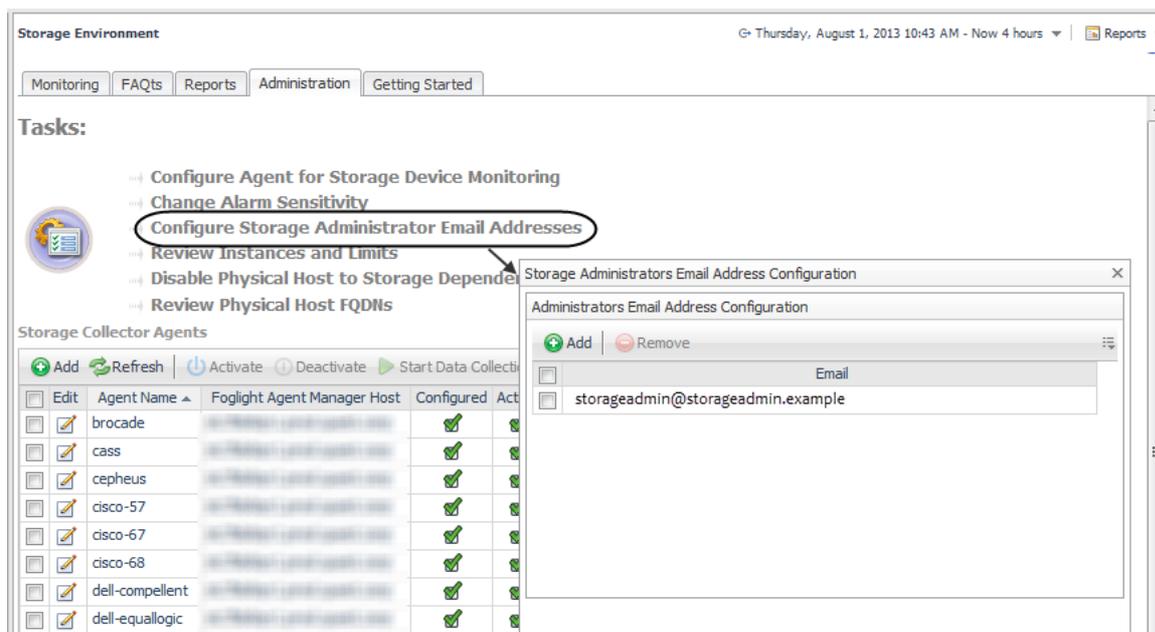
Troubleshooting Database Limits

Foglight for Storage Management sets limits on the number of instances of each object type that can exist in the Database Repository. On the Administration tab, the Review Instances and Limits task enables you to view a table containing a list of Foglight for Storage Management object types.

For each object type, the table displays the instance limit, the number of instances currently in the database, the utilization (count/limit), and a status based on utilization. While the utilization remains below 90%, the object type status is Normal. When utilization reaches 90%, the status becomes Critical; if you intend to monitor new instances of this object type, you should take some steps to plan for the growth. At 100%, the status changes to Fatal and Foglight for Storage Management does not create anymore instances of the object type. For example, if the SanLUN object type is at 99% utilization, and you add an agent to monitor a new storage array that has 200 LUNs configured, the SanLUN instance limit will soon be reached and you will not see data for many of the new LUNs in the dashboards.

The limit on the number of instances per object type is a global default value, which is set in the registry variable called *foglight.limit instances*. You can override the limit for selected topology types.

> ! **CAUTION: Before changing limits, you may want to consult with a Support Engineer to discuss alternatives. You want to ensure that the size of your database remains reasonable while still meeting your monitoring requirements.**

To review the number of instances of each Storage object type in the Foglight for Storage Management database:

1   On the Storage Environment dashboard, in the **Administration** tab, click **Review Instances and Limits**.

Edit Registry Variables				
Object Type	Instance Limit	Instance Count	Utilized ▾	Status
SanLinkDependency2	50,000	627	1.3 %	✓
SanPhysicalDisk	50,000	423	0.8 %	✓
SanFcSwitchPort	50,000	392	0.8 %	✓
SanLun	51,000	347	0.7 %	✓
SanFcAttachedPort	50,000	253	0.5 %	✓
SanVolumeExportName	50,000	179	0.4 %	✓
SanVolume	50,000	58	0.1 %	✓
SanPool	50,000	42	0.1 %	✓
SanStorageSupplierPortFC	50,000	36	0.1 %	✓
SanStorageSupplierPortISCSI	50,000	34	0.1 %	✓
SanLinks	50,000	18	0.0 %	✓
SanFcSwitch	50,000	17	0.0 %	✓
SanAgentMessage	50,000	16	0.0 %	✓
SanController	50,000	14	0.0 %	✓
SanStorageSupplierPortIB	50,000	13	0.0 %	✓
SanDirExportName	50,000	10	0.0 %	✓
SanVolumeDir	50,000	10	0.0 %	✓
SanMember	50,000	9	0.0 %	✓
SanStorageArray	50,000	8	0.0 %	✓
SanVsan	50,000	5	0.0 %	✓
SanISLLinks	50,000	5	0.0 %	✓
SanFabric	50,000	5	0.0 %	✓
SanFiler	50,000	4	0.0 %	✓
SanSale	50,000	0	0.0 %	✓

2   Review the Status column. If any of the icons are Critical or Fatal, consider either modifying how you monitor that type of object or extending the limit for that object type.

3   To increase or decrease a limit, click **Edit Registry Variables** and select **foglight.limit.instances**.

On the Edit Registry Variables dashboard, open the online help to learn how to add a registry variable for an object type and set its instance limit.

Understanding Metrics

This section defines the metrics displayed in the Storage & SAN dashboards. It also provides an overview of metrics in Foglight for Storage Management—you need this information if you intend to create new rules or custom dashboards.

This section contains the following topics:

- Units of Measurement
- Performance Metrics
- Capacity Metrics
- Overview of Metrics in Foglight for Storage Management

Units of Measurement

Foglight for Storage Management uses the following units of measurement:

- **B/s** — Number of bytes per second. Frequently converted to KB/s or MB/s.
- **ops/s** — Number of operations per second.
- **ms** — Milliseconds. Frequently converted to μs (microsecond).
- **m** — milli — Thousandth.
- **ms/op** — Milliseconds per operation.
- **MB** — Capacity metrics are captured in MB (megabytes), but are frequently displayed in GB (gigabytes) or TB (terabytes).

Performance Metrics

In general, performance is gauged in terms of rates (such as data rates, ops to disk rates, frame rates), latency, and utilization. The selection of performance metrics displayed in any given dashboard depends on the selected device type and the metrics available from the device vendor.

The following tables define each metric and shows the topology name for the metric. You need the topology name when referencing the metric in user-defined rules and dashboards.

Performance metrics are organized into the following categories:

- Fabrics and FC Switches — Performance Metrics
- Storage Arrays and Filers — Disk I/O Performance Metrics
- Clustered Storage Arrays — Network Performance Metrics

Fabrics and FC Switches — Performance Metrics

For fabrics and switches, performance is assessed in terms of send and receive values for the FC switch ports and is expressed as the average number of bytes per second or frames per second. Port errors are also an important indicator of port performance, because a higher number of errors correlates with lower send and receive values.

Table 21. Performance metrics

Display Name	Description	Topology Name
Baseline	A range of normal values, as determined by IntelliProfile by looking at historical data for the same time range. A baseline range displays after seven days of data collection.	*n/a*
Data Rate	Bytes per second sent and received though a port.	bytesTotal
Data Receive Rate	Average number of bytes per second received through a port. The data rate, compared against the Baseline of typical activity, indicates whether the current traffic is typical or out of the norm.	bytesRcvd
Data Send Rate	Also **Data Xmit Rate** Average number of bytes per second transmitted through a port. The data rate, compared against the Baseline of typical activity, indicates whether the current traffic is typical or out of the norm.	bytesXmit
Frame Rate	Average number of frames per second received and transmitted through a port.	framesTotal
Frame Receive Rate	Average number of frames per second received through a port.	framesRcvd
Frame Send Rate	Also **Frame Xmit Rate** Average number of frames per second transmitted through a port.	framesXmit
Link Error Rate	Average number of link errors *per second* on a port. Link errors are caused by or affect the link status of the connection. Link errors include: • Link resets • Loss of signal on the port • Loss of synchronization If an error rate value is very small, it may be displayed as 0.0. If a fabric or switch has an actual error rate of 0, it is not displayed.	errorsLink
Link Speed	Current speed of a port in Mb/second.	currentSpeedMb
Non-Link Error Rate	Average number of non-link errors *per frame* on a port. Non-link errors include: • Resource constraint that causes frames to be retried • CRC errors • Frame length errors • Address errors If an error rate value is very small, it may be displayed as 0.0. If a fabric or switch has an actual error rate of 0, it is not displayed.	nonLinkErrors

Table 21. Performance metrics

Display Name	Description	Topology Name
Rcvd Utilization	= Data Receive Rate / Link Speed, expressed as a percentage. Utilization values help you identify ports that may be overloaded.	bytesRcvd Utilization
Xmit Utilization	= Data Send Rate / Link Speed, expressed as a percentage. Utilization values help you identify ports that may be overloaded.	bytesXmit Utilization

Storage Arrays and Filers — Disk I/O Performance Metrics

Rate and latency metrics describe the performance of ports, controllers, pools, LUNs, disks, and NASVolumes. The selection of performance metrics displayed in any given dashboard depends on the selected device type and the metrics available from the device vendor.

> **i** | **NOTE:** For controllers, the Date Rate, Latency, and Ops Rate sets of metrics include Block and File versions as well to track block and file operations separately. For example, Data Rate has Data Rate (File) and Data Rate (Block). These sets of metrics are not included in this table.

Table 22. Disk I/O Performance Metrics

Display Name	Description	Topology Name
% Busy	Also displayed as **Pct Busy** or **Busiest** Average percentage of time a component is busy doing I/O during the collection period.	busy
Average Queue Depth	Average number of outstanding I/O operations at the start of each new I/O request in a pool, LUN, or disk.	avgQueueDepth
Cache Hit Rate	Percentage of read operations that can be satisfied from the cache.	cacheHits
L1 Cache Hit Rate	Percentage of read operations that can be satisfied from this cache.	cacheHitRate_L1
L2 Cache Hit Rate	Percentage of read operations that can be satisfied from this cache.	cacheHitRate_L2
Data Rate	Bytes per second read and written.	bytesTotal
Data Read Rate	Bytes per second read.	bytesRead
Data Write Rate	Bytes per second written.	bytesWrite
Disk Latency	Average latency for read/write operations to the disks in a pool, calculated in milliseconds per operation. At the pool level, Avg Disk Latency reflects the average latency for I/O to the physical disks.	latencyTotalDisk
Latency (R/W Latency)	Average latency for read/write operations, calculated in milliseconds per operation. At the pool level, Latency reflects I/O to the pool only. If the block of data to be read is already in a cache, then the latency for that operation is very low, because no disk access needs to be performed. **NOTE:** Latency is *not* the sum of read latency and write latency. The number of read operations and write operations is different.	latencyTotal
Other Latency	Average latency for other operations	latencyOther
Read Latency	Average latency for read operations.	latencyRead

Table 22. Disk I/O Performance Metrics

Display Name	Description	Topology Name
Write Latency	Average latency for write operations.	latencyWrite
Ops Rate	Average read and write operations per second.	opsTotal
Read Ops Rate	Read operations per second.	opsRead
Write Ops Rate	Write operations per second.	opsWrite
Other Ops Rate	Other operations per second.	opsOther

Clustered Storage Arrays — Network Performance Metrics

These metrics describe the performance of an EqualLogic array's network and an Isilon array's internal and external networks.

Table 23. Network Performance Metrics

Display Name	Description	Topology Name
Link Speed	Current operational speed of the port link.	currentSpeedMb
Max Port Speed	Rated maximum speed of the port	maxSpeedMb
Packet Errors %	Number of incorrectly received data packets divided by the total number of received packets, expressed as a percentage.	packetErrorPercent
Rcv Data Rate	Bytes per second received through a port or group of ports.	bytesWrite
Send Data Rate	Bytes per second sent through a port or group of ports.	bytesRead
Rcv Util	= Rcv Data Rate / Link Speed	bytesWrite Utilization
Send Util	= Send Data Rate / Link Speed	bytesRead Utilization
Rcv Util (% of max)	Also **NW Rcv Util (% of max)** = Rcv Data Rate / Max Port Speed	bytesWrite UtilizationMax
Send Util (% of max)	Also **NW Send Util (% of max)** = Send Data Rate / Max Port Speed	bytesRead UtilizationMax

Capacity Metrics

The selection of capacity metrics displayed in any given dashboard depends on the selected device type and the metrics available from the device vendor. The following tables define each metric and shows the topology name for the metric. You need the topology name when referencing the metric in user-defined rules and dashboards.

Capacity metrics are organized into the following categories:

- Storage Arrays — Array, Member, and Pool Capacity Metrics
- Filers — Filer and Aggregate Capacity Metrics
- Storage Arrays and Filers — LUN, NASVolume, and Disk Capacity Metrics

Storage Arrays — Array, Member, and Pool Capacity Metrics

The following table contains the capacity metrics you may see displayed for storage arrays, members/nodes, and pools.

> **NOTE:** To view the metrics for EMC Isilon arrays (which are significantly different than other arrays), see EMC Isilon Only Capacity Metrics.

Table 24. Array, Member, and Pool Capacity Metrics

Capacity Metric	Description	Array	Member/Node	Pool	Topology Name
Total Advertised LUNs Size	Also **Advertised LUNs Size** Sum of the Advertised LUN Size for all LUNs in the entity.	✅		✅	conf_LunSize
Available Raw Capacity	Capacity available in the pool that has not been committed to data, snapshots, or thick-provisioned LUNs. Raw counts all the disk blocks available, before applying RAID.			✅	raw_available
Available Usable Capacity	Also **Available Capacity** Capacity available in the pool that has not been committed to data, snapshots, or thick-provisioned LUNs. *Usable* means after applying RAID.			✅	conf_available
Capacity Provisioned to LUNs	Also **Provisioned to LUNs** Capacity used for LUN data. Does not include capacity that is used for snapshots, reserves, etc. • For thin-provisioned LUNs, this is the capacity used for data written to the LUNs. • For thick-provisioned LUNs, this is the capacity allocated to the LUNs, and does not reflect data written *Formerly displayed as Consumed Capacity*.	✅		✅	*Array*: lun_usable_capacity *Pool*: conf_used
Overcommitment	= Total Advertised LUNs Size – Total Usable Capacity Overcommitment reflects the minimum additional capacity needed in the pool to support the advertised capacity promised to thin-provisioned LUNs. When the value of overcommitment is greater than zero, you run the risk of I/O writes failing because of insufficient physical storage to support the demand. Overcommitment is available only for arrays where the vendor provides the total usable capacity.	✅		✅	conf_LunOvercommitted

Table 24. Array, Member, and Pool Capacity Metrics

Capacity Metric	Description	Array	Member/Node	Pool	Topology Name
Total Disk Capacity	Sum of the sizes of the disks in the array. This includes spares.	✓			disk_capacity
Total Raw Capacity	Total capacity of the pool in raw terms. Raw counts all the disk blocks allocated to the pool, before applying RAID.			✓	raw_capacity
Total Usable Capacity	Total capacity of the pool or member/node in usable terms. Pools that are defined with a specific RAID level have this metric. Pools that can support LUNs with different RAID levels do not have this metric.		✓	✓	conf_capacity
Used Capacity	= Total Usable Capacity - Available Usable Capacity.		✓		conf_used
% Used	= Used Capacity / Total Usable Capacity Percentage of the member/node's usable capacity that has been used.		✓		*Calculated*
% of Pool	*EqualLogic Pools-Members tab only.* Percentage of the pool storage capacity provided by a pool member.		✓		*Calculated*

EMC Isilon Only Capacity Metrics

Isilon arrays provide additional metrics to describe the Isilon OneFS file system (IFS) capacity in terms of hard disk drive (HDD) and solid state drive (SSD) capacity.

Table 25. EMC Isilon only Capacity Metrics

Capacity Metric	Description	Array	Member/Node	Pool	Topology Name
Total HDD Capacity	Raw capacity of the hard drives in the array, as reported by the vendor.	✓			raw_capacity_HDD
Total SSD Capacity	Raw capacity of the solid-state drives in the array, as reported by the vendor.	✓			raw_capacity_SSD
IFS Capacity: Total	Total capacity of the Isilon File System.	✓		✓	*Array*: pool_capacity_conf *Pool*: conf_capacity
IFS Capacity	= Total HDD Capacity + Total SSD Capacity Capacity of the Isilon File System on a pool or member/node.		✓	✓	conf_capacity
IFS Capacity: Free	Also **IFS Free** Free capacity of Isilon File system.	✓	✓	✓	*Array*: pool_free_conf *Pool and member*: conf_available

Table 25. EMC Isilon only Capacity Metrics

Capacity Metric	Description	Array	Member/Node	Pool	Topology Name
IFS Capacity Used	= IFS Capacity - IFS Capacity: Free	✓	✓	✓	*Calculated*
IFS Capacity: HDD Total	Capacity of Isilon File System on hard disk drives in an array, pool, or node.	✓	✓	✓	conf_capacity_HDD
IFS Capacity: HDD Free	Free capacity of Isilon File System on hard disk drives in an array, pool, or node.	✓	✓	✓	conf_available_HDD
IFS Capacity: HDD Used	= IFS Capacity: HDD Total - IFS Capacity: HDD Free	✓	✓	✓	*Calculated*
IFS Capacity: SDD Total	Capacity of Isilon File System on solid state drives in an array, pool, or node.	✓	✓	✓	conf_capacity_SSD
IFS Capacity: SDD Free	Free capacity of Isilon File System on solid state drives in an array, pool, or node.	✓	✓	✓	conf_available_SSD
IFS Capacity: SDD Used	= IFS Capacity: SDD Total - IFS Capacity: SDD Free	✓	✓	✓	*Calculated*
HDD % Free	= IFS Capacity: HDD Free / IFS Capacity: HDD Total		✓	✓	conf_pct_available_ HDD
SDD % Free	= IFS Capacity: SDD Free / IFS Capacity: SDD Total		✓	✓	conf_pct_available_ SSD

Filers — Filer and Aggregate Capacity Metrics

Foglight for Storage Management supports NetApp filers (**F**). NetApp uses the word *aggregate* (**Ag**) instead of pool, but the metrics collected for aggregates are similar to the metrics collected for pools.

Table 26. Filer and Aggregate Capacity Metrics

Capacity Metric	Description	Filer	Aggregate	Topology Name
Advertised LUNs Size	Also **Total Advertised LUNs Size** or **Adv LUNs Size** Sum of the Advertised LUN Size for all LUNs in the entity.	✓		configured_lun_size
Advertised NASVolumes Size	Sum of the Advertised Size for all NASVolumes.	✓	✓	*Filer*: configured_vol_size *Aggregate*: conf_VolSize
Disk Capacity (Raw)	Also **Total Disk Capacity** Sum of the sizes of the disks in the filer. This includes spares.	✓		disk_capacity

Table 26. Filer and Aggregate Capacity Metrics

Capacity Metric	Description	Filer	Aggregate	Topology Name
Free Disk/Spares Capacity (Raw)	Amount of disk capacity that has not been committed to an aggregate. Disk capacity cylinder coloring and capacity alarms are defined in registry variables with the prefix: *StSAN.FilerDisks.PctUnallocatedCapacityThreshold...*	✅		disk_free
Aggr Capacity (Usable) Total	Also **Total Usable Aggr Capacity** Sum of the Total Usable Capacity of all the aggregates in the filer. Aggregate capacity cylinder coloring and alarms are defined in registry variables with the prefix: *StSAN.FilerAggregates.PctUnallocatedCapacity Threshold...*	✅		pool_capacity_conf
Aggr Capacity (Usable) Free	Also **Available Aggr Capacity** Sum of the Available Usable Capacity in the aggregates. Usable means after applying RAID.	✅		pool_free_conf
Aggr Capacity (Raw) Total	Also displayed as **Aggregate Capacity (Raw)** Sum of the raw capacity of all the aggregates in the filer.	✅		pool_capacity_raw
Aggr Capacity (Raw) Free	Sum of the available raw capacity in all the aggregates.	✅		pool_free_raw
Overcommitment	= Advertised NASVolumes Size – Aggr Capacity (Usable) Total Overcommitment reflects the minimum additional capacity needed in the aggregate to support the advertised capacity promised to thin-provisioned volumes and LUNs. When the value of overcommitment is greater than zero, you run the risk of I/O writes failing because of insufficient physical storage to support the demand.		✅	conf_overcommitted
Total Usable Capacity	Total capacity of the aggregate in usable terms. Usable means after applying RAID.		✅	conf_capacity
Available Usable Capacity	Also displayed as **Available Capacity** Capacity available in the aggregate that has not been committed to data, snapshots, or thick-provisioned volumes and LUNs, in usable terms. Usable means after applying RAID.		✅	conf_available
Used Capacity	= Total Usable Capacity – Available Usable Capacity		✅	conf_used
% Available	Also **% Free** = Available Usable Capacity / Total Usable Capacity		✅	*Calculated*

Storage Arrays and Filers — LUN, NASVolume, and Disk Capacity Metrics

These metrics describe the capacity of LUNs, NASVolumes, and disks.

Table 27. LUN, NASVolume, and Disk Capacity Metrics

Capacity Metric	Description	LUN	NASVolum	Disk	Topology Name
Advertised LUN Size	Size of the LUN as advertised to the hosts connected to the LUN.	✅			advertisedSize
Provisioned Usable Capacity	Capacity provisioned for LUN data. In a thin-provisioned LUN, this is the capacity used for data written to the LUN. In a thick-provisioned LUN, this is the capacity allocated to the LUN, and does not reflect data written.	✅			size
Provisioned Raw Capacity	Capacity provisioned for LUN data in raw terms.	✅			rawCapacity
Advertised Size	Size of the NASVolume as advertised to the host mounting the volume.		✅		total_capacity
Free Capacity	Advertised Size – Used Capacity		✅		available_capacity
Used Capacity	Capacity in volume committed to data, snapshots, etc. in usable terms.		✅		used_capacity
% Used	= Used Capacity / Advertised Size		✅		percent_used
Disk Size	Size of the disk in MBs. Disk capacity cylinder coloring and capacity alarms are defined in registry variables with the prefix: *StSAN.FilerDisks.PctUnallocatedCapacityThreshold...*			✅	size

Overview of Metrics in Foglight for Storage Management

Metrics and data are saved in the Foglight for Storage Management database as properties of topology objects. Topology objects correspond to the types of storage devices and components being monitored in your storage environment.

ℹ | **TIP:** For in-depth information about the Foglight for Storage Management data model, see the *Data Model Guide*.

Summary of SAN Topology Objects

If you want to create new rules or custom dashboards, or if you want to browse the data directly instead of through the Storage & SAN dashboards, you need to know the names of devices, components, and metrics as they are stored in the Foglight for Storage Management Database Repository.

The following tables list the top-level storage devices and all child components, and identifies their topology object names. These lists are not comprehensive, rather they reflect the objects that you may need to reference if you are creating new rules or custom dashboards. For other objects, see the Data dashboard. For help navigating to the Data dashboard, see Locating SAN Topology Objects in Foglight for Storage Management.

Table 28. SAN Topology Objects

Device	Topology Object
Fabric	`SanFabric`
Fibre Channel Switch	`SanFcSwitch`
VSAN	`SanVsan`
Filer	`SanFiler`
Storage Array	`SanStorageArray`

Component	Topology Object
FC Switch Port	`SanFcSwitchPort`
FC Port (Arrays/Filers)	`SanStorageSupplierPortFC`
IP Port (Arrays/Filers)	`SanStorageSupplierPortISCSI`
InfiniBand Port (Arrays)	`SanStorageSupplierPortIB`
Controller	`SanController`
Disk	`SanPhysicalDisk`
LUN	`SanLun`
Member	`SanMember`
NASVolume	`SanVolume`
Pool or Aggregate	`SanPool`
Virtual Machine	`SanStorageVirtualMachine`
Logical Interface	`SanLogicalInterface`

Locating SAN Topology Objects in Foglight for Storage Management

ℹ️ | **NOTE:** You require the Foglight for Storage Management role *Administrator* to access the Configuration > Data menu.

You can explore directly the metrics and data captured for monitored storage devices and their components. Data is displayed as a hierarchy of objects.

To locate storage topology objects:

1. On the navigation panel, under Dashboards, click **Configuration > Data**.

2. Expand the **Storage & SAN** branch.

3. Select a device type and then a device.

4. Select a metric to view details in the Property Viewer.

For example, the following image shows a selected FC Switch (brocade3900_3). The Data Rate metric, which is called `bytesRcvd`, is selected and displayed in the Property Viewer. The Property Viewer contains tables showing all collected values for the selected metric. For more information, see Understanding Metric Data in Charts and Tables.

Figure 20. Property Viewer

Appendix: Supported Storage Devices Table

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

Table 29. 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) **NOTE:** Metro Cluster is not supported.	DATA ONTAP 8.X up to 9.6
Storage Arrays	**Dell Compellent**	Dell Enterprise Manager (EM)	EM 2015 R3 (Build 15.3.1.300)
		Dell Storage Manager (DSM)	DSM 2018 R1
	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	• 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	• 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 and Metro	GeoSynchrony 6.0 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 HP 3PAR StoreServ 8000 HP 3PAR StoreServ 8400	N/A

Table 29. Support matrix

		Supported platforms	Supported latest GA
Generic SMI-S Array	**Dot Hill**	Dothill Assured SAN 5720 (Seagate)	N/A
	EMC Unity	Unity 300/300F	N/A
		Unity 400/400F	N/A
		Unity 500/500F	N/A
		Unity 600/600F	N/A
		UnityVSA	N/A
	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 V5 Series	V5R7 and later
		OceanStor Dorado	V3, V3R1, and V6 Series
	PureStorage	FA-420	N/A
	IBM	StoreWize v3700	N/A
	Lenovo	Lenovo DS4200	N/A

About Us

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.