

Foglight™ APM 5.9.8

User Guide



© 2015 Dell Inc.
ALL RIGHTS RESERVED.

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

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

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

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (software.dell.com) for regional and international office information.

Patents

This product is protected by U.S. Patents # 6,928,471; 7,539,655; 7,565,336; 7,941,385; 7,979,245; 8,175,862; 8,175,863; and 8,892,415. Additional Patents Pending.

For more information, go to <http://software.dell.com/legal/patents.aspx>.

Trademarks

Dell, the Dell logo, Foglight, IntelliProfile, NetVault, PerformaSure, PowerEdge, and Tag and Follow are trademarks of Dell Inc. "Apache HTTP Server", Apache, "Apache Tomcat" and "Tomcat" are trademarks of the Apache Software Foundation. Google is a registered trademark of Google Inc. Chrome, Android, and Nexus are trademarks of Google Inc. Red Hat, JBoss, the JBoss logo, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries. CentOS is a trademark of Red Hat, Inc. in the U.S. and other countries. Microsoft, .NET, Active Directory, Internet Explorer, Hyper-V, SharePoint, SQL Server, Windows, Windows Vista and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. AIX, IBM, PowerVM and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Sun, Oracle, Java, Oracle Solaris, and WebLogic are trademarks or registered trademarks of Oracle and/or its affiliates in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries. Products bearing the SPARC trademarks are based on an architecture developed by Oracle Corporation. OpenLDAP is a registered trademark of the OpenLDAP Foundation. HP is a registered trademark that belongs to Hewlett-Packard Development Company, L.P. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries. Novell and eDirectory are registered trademarks of Novell, Inc., in the United States and other countries. VMware, ESX, ESXi, vSphere, vCenter, vMotion, and vCloud Director are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Sybase is a registered trademark of Sybase, Inc. The X Window System and UNIX are registered trademarks of The Open Group. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. "Eclipse", "Eclipse Foundation Member", "EclipseCon", "Eclipse Summit", "Built on Eclipse", "Eclipse Ready", "Eclipse Incubation", and "Eclipse Proposals" are trademarks of Eclipse Foundation, Inc. IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Apple, iPad, iPhone, Mac OS, Safari, Swift, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Ubuntu is a registered trademark of Canonical Ltd. Symantec and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. YAST is a registered trademark of SUSE LLC in the United States and other countries. Citrix, AppFlow, NetScaler, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. AlertSite and DéjàClick are either trademarks or registered trademarks of Boca Internet Technologies, Inc. Samsung, Galaxy S, and Galaxy Note are registered trademarks of Samsung Electronics America, Inc. and/or its related entities. MOTOROLA is a registered trademark of Motorola Trademark Holdings, LLC. The Trademark BlackBerry Bold is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Dell is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited. Ixia and the Ixia four-petal logo are registered trademarks or trademarks of Ixia. Opera, Opera Mini, and the O logo are trademarks of Opera Software ASA. Tevron, the Tevron logo, and CitraTest are registered trademarks of Tevron, LLC. PostgreSQL is a registered trademark of the PostgreSQL Global Development Group. MariaDB is a trademark or registered trademark of MariaDB Corporation Ab in the European Union and United States of America and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest

in the marks and names of others.

Legend

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

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

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

Foglight APM User Guide
Updated - June 2015
Foglight APM Version - 5.9.8

Contents

Getting started with Foglight APM	7
Introducing APM	7
Who uses Foglight APM	7
Finding the Foglight APM dashboards	8
Getting started with Foglight APM	8
Monitoring transactions	10
Investigating real user APM transactions	12
Investigating application server transactions	14
Configuring display options	16
Viewing real user activity from a geographical perspective	18
Assessing real user experiences during key sequences	23
Introducing the Sequence Explorer dashboard	23
Investigating sequence activity	25
Investigating Event tiles details	27
Changing the timeslice and the time range	28
Creating custom Sequence Explorer dashboards	29
Monitoring the performance of web sites and endpoints	30
Introducing the Web Sites and Endpoints dashboard	30
Exploring the top busiest web sites or endpoints	32
Exploring alarms on web sites or endpoints	32
Investigating a web site or endpoint	33
Troubleshooting an excessive number of monitored web sites	35
Searching APM data	36
Searching and investigating hits	36
Defining simple searches for hits	37
Defining expert searches for hits	37
Understanding search hits results	38
Investigating hit results	40
Searching and investigating sessions	42
Defining simple searches for sessions	43
Defining expert searches for sessions	44
Understanding search sessions results	45
Investigating issues reported during real user sessions	47
Searching and investigating sequences	50
Defining simple searches for sequences	51
Defining expert searches for sequences	51
Understanding search sequences results	53
Investigating sequence results	54
Managing searches	55

Repeating the last search	55
Saving searches	55
Running saved searches	56
Clearing search results	56
Defining match conditions for expert searches	56
Replaying sessions, hits, and sequences	58
Introducing the Replay browser	58
Changing how content is displayed	60
Customizing the Selection pane	60
Understanding what happens when content is unavailable	61
Using the Hit Inspector	61
Managing saved sessions	62
Saving sessions	62
Exporting sessions	63
Importing sessions	63
Replaying saved sessions	64
Visualizing search results	65
Viewing search results in a map	65
Viewing search results in pivot charts	67
Publishing maps and charts to custom dashboards	68
Publishing maps and charts	68
Adding maps or charts to a custom dashboard	69
Managing published maps and charts	71
Creating custom drag-and-drop dashboards	72
Linking a custom dashboard to the Explore icon for a service	80
APM tile and view reference	82
Overview of APM tiles	83
Application Servers - .NET tile	84
.NET tile	85
Application Servers - Java tile	86
DB2 tile	87
Host tile	87
JMX tile	88
MQ tile	89
Oracle tile	89
OS tiles	90
Server - Apache Monitor tile	91
Application Monitor tile	91
Log Filter tile	92
Web Monitor tile	92
Pivot tiles	93
Real User (APM) tile	94
Real User (FxM) tile	95

Sequence tile96
SQL Server tile97
Sybase tile97
Synthetics tile98
Multi-Location Synthetics tile98
Single-Location Synthetics tile99
Virtual Hyper-V tile	100
VMware tile	101
Overview of Detail views	102
Application Server detail view	102
Host detail view	103
Pivot Breakdown detail view	103
Real User (APM) Performance detail view	104
Hits and Pages tabs	104
Response Time Breakdown tab	105
Application Infrastructure tab	107
Related Infrastructure tab	107
Real User (FxM) Performance detail view	108
Performance tab	108
Response Time Breakdown tab	110
SLA Violators tab	111
Synthetic Result detail view	112
Synthetic User Performance detail view	113
Virtual Machine detail view	114
ESX Server detail view	114
Topology object name reference table	115
Contacting Dell	117
Technical support resources	117

Getting started with Foglight APM

Foglight™ APM for Real User Experience (hereafter called Foglight APM) is an appliance-based application performance management solution. This *User Guide* walks you through using top-level APM dashboards to assess the experiences of your real end users as they navigate your monitored web sites and web applications.

Using this guide you can also learn how to create powerful, flexible searches to retrieve details directly from the Archiver database, enabling you to find answers to questions you have about your real users, and also to respond to any problems reported by real end users. From search results, you can replay hits, sequences, and sessions. You can also visualize aggregated details and metrics in maps and pivot charts. This guide is intended for Foglight users with the role of APM Operator or APM Administrator.

If you are new to application performance monitoring (APM), review the first two sections of this section for a quick introduction to APM. The rest of the section tells you how to find the APM dashboards in Foglight and which dashboards to look at first.

NOTE: This guide focuses on the real user experience and web request monitoring features included in Foglight APM. If you want to know more about Java™ and .NET® monitoring functionality, see the *Foglight for Application Operations User and Reference Guide*.

This section introduces you to Foglight APM through the following topics:

- [Introducing APM](#)
- [Who uses Foglight APM](#)
- [Finding the Foglight APM dashboards](#)
- [Getting started with Foglight APM](#)

Introducing APM

Application performance monitoring (APM) refers to a set of capabilities or technologies used by IT staff to support the incident and problem management processes on multi-tier applications. A comprehensive APM implementation generally includes technology that provides the following capabilities:

- Real user experience monitoring
- Run-time application topology and execution path discovery, modeling, and display
- Transaction profiling across the technology stack
- Resource consumption and event monitoring within the discovered components
- Analytics

Foglight APM supports all these capabilities, and provides information to the right users at the right time through a set of role-oriented operational dashboards.

Who uses Foglight APM

Although there is no single organizational alignment or uniformly agreed upon set of titles for the actual practitioners of APM, the following list identifies the some of the people who typically use Foglight APM:

- *Application Support* – responsible for ensuring that application services are performing as expected. Identifies and triages service degradations or outages.
- *Platform Specialist or Administrator* – responsible for the operation of an individual application component (for example, a database, a host, an application server, or a web server). Receives and responds to Foglight alarms on their platform or domain.
- *Application Architect* – a senior escalation resource who is typically engaged by Application Support for assistance in locating the source of an application issue.
- *Application Developer* – responsible for the application code. Uses the Foglight transactional performance dashboards to gain an understanding of the operational execution and performance of their code.

In addition, a Foglight APM solution requires that one or more people take on responsibilities to design, implement, and maintain the solution. These people perform the following functions:

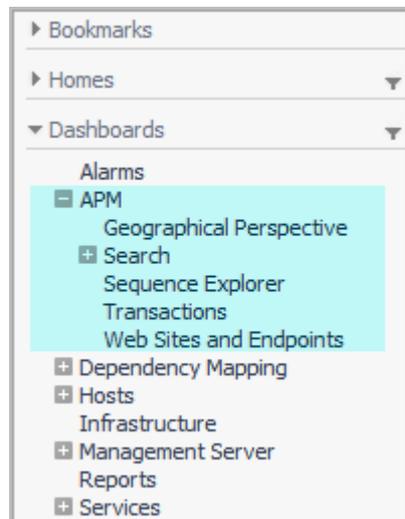
- *Application Performance Manager* – designs and executes the APM strategy. Decides which of the organization’s web sites and web applications to monitor.
- *Foglight APM Administrator (Foglight role)* – configures Foglight to monitor web traffic for the selected web sites and web applications.
- *Foglight Administrator (Foglight role)* – configures and manages Foglight, and performs administrative tasks, such as assigning user roles.

The Foglight APM Administrator assigns the role of APM Operator to everyone who needs access to the APM dashboards to evaluate real user activity.

Finding the Foglight APM dashboards

To find the Foglight APM dashboards, in the Foglight navigation panel, under Dashboards, expand **APM**. Top-level APM dashboards enable you to view aggregated data by sequence, transaction, or geographical perspective. The Search dashboards enable you to search the Archiver database by hits, sessions, or sequences.

Figure 1. The APM dashboard menu.



The APM menu contains the following menu items:

Geographical Perspective – assess the performance of your web sites and applications by city, country, or region.

Search – search the Archiver databases for details about hits, sequences, and sessions.

Sequence Explorer – assess the performance of important workflows in your web applications.

Transactions – monitor real user experiences with or without the other transactional data captured by Foglight.

Web Site and Endpoints – assess the performance of your web sites and endpoints.

Getting started with Foglight APM

You can start assessing your real user experiences of your monitored web sites and web applications using any of the APM dashboards. Depending on your job function, however, you may be more interested in some results than others. The following table lists common getting started tasks, the dashboard to use, and the people who primarily use the dashboard.

TIP: If you are not seeing data for a web site or web application, ask the person with the Application Performance Manager function in your organization to consider monitoring the site/application.

Table 1. Common “getting started” tasks

Task	APM dashboard	Job functions	For information, see
Monitor real user activity on your sites and applications. Investigate alarms and any tiles with a non-normal status.	Transactions	<ul style="list-style-type: none"> Application Support Platform Specialist or Administrator 	Monitoring transactions
Find out the locations where your site or application performs well/poorly or experiences high/low volume. NOTE: Displays data only when an APM Administrator enables mapping on selected hit analyzers.	Geographical Perspective	<ul style="list-style-type: none"> Application Support Application Architect 	Viewing real user activity from a geographical perspective
Assess the health of your sites and applications as well as all the monitored endpoints (server + port). Investigate alarms and any tiles with a non-normal status.	Web Sites and Endpoints	<ul style="list-style-type: none"> Application Support Developers Network Administrators 	Monitoring the performance of web sites and endpoints
If a real user reports having issues with your web site, you can search for the session and replay it to see what your user experienced.	Search	<ul style="list-style-type: none"> Application Support Application Architect 	Searching APM data
Monitor critical paths in your sites and applications. NOTE: Displays data only when an APM Administrator defines sequence analyzers to identify the series of events to track.	Sequences	<ul style="list-style-type: none"> Any 	Assessing real user experiences during key sequences

Monitoring transactions

A transaction occurs when a user or synthetic robot makes a request to a monitored application. Depending on the components in your installation, Foglight APM can capture and correlate transactional activity at multiple layers including:

- Real/synthetic user behavior
- Web requests and responses
- Web servers and application servers
- Application code execution
- Database I/O
- Operating systems
- Physical and virtual servers

With the Transactions dashboard, you can examine transactional data in the following ways:

- Fully-linked end-user to database transactions
- End-user transactions only (synthetic or real) aggregated by location or other details
- Application layer transactions only (Java™ EE or .NET®)

The tiles on the Transactions dashboard represent different transactional views. Use the table below to quickly determine the type of transaction, then review [Investigating real user APM transactions](#) for an overview of how to drill down for more information.

Transaction type icons

Table 2. Transaction type icons and links to full descriptions

Icon	Transaction Type
	Foglight APM for Real User Experience transaction. For more information, see Real User (APM) Performance detail view .
	Foglight Experience Monitor/Viewer End User transaction. For more information, see Real User (FxM) Performance detail view .
	Foglight for Java EE Technologies or Foglight for Microsoft .NET transaction. For more information, see Application Server detail view .
	Foglight Transaction Recorder Synthetic User transaction. For more information, see Synthetic Result detail view .
	Sequence. For more information, see Sequence tile .

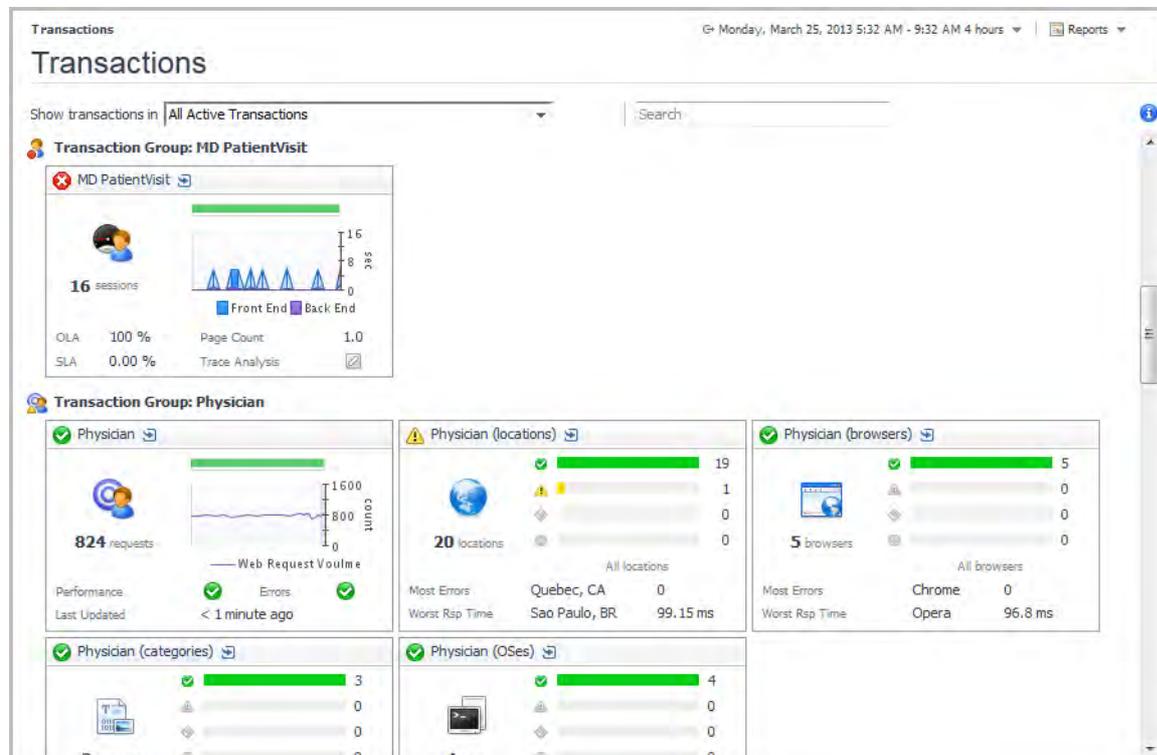
Table 2. Transaction type icons and links to full descriptions

Icon	Transaction Type
	Pivot - Browsers. For more information, see Pivot tiles .
	Pivot - Content Types. For more information, see Pivot tiles .
	Pivot - Endpoints. For more information, see Pivot tiles .
	Pivot - Locations. For more information, see Pivot tiles .
	Pivot - OSes. For more information, see Pivot tiles .

For example, in the following image, the *Physician* group of tiles represents a real user perspective with pivot data. The performance summary on each tile includes an alarm state overview and other key metrics. For a full description of the metrics displayed on each type of tile, see [APM tile and view reference](#).

NOTE: If some of the transactional data that you want to investigate is not available in your installation, you may need to install and configure additional Foglight components, such as Foglight for Java EE Technologies.

Figure 2. The Transactions dashboard in Foglight.



For more information, see the following topics:

- [Investigating real user APM transactions](#)
- [Investigating application server transactions](#)
- [Configuring display options](#)

Investigating real user APM transactions

The Transactions dashboard enables you to quickly identify if any transactions are having issues, to determine the magnitude of impact on the user population, and to view preliminary information that can aid in troubleshooting, including geographic discrepancies and whether the performance problems are in the back-end architecture, or the client-side browser or network.

- ① **TIP:** The Service Operations Console includes a Transaction tab that displays transactions as services. The investigative workflow is similar to that described here.

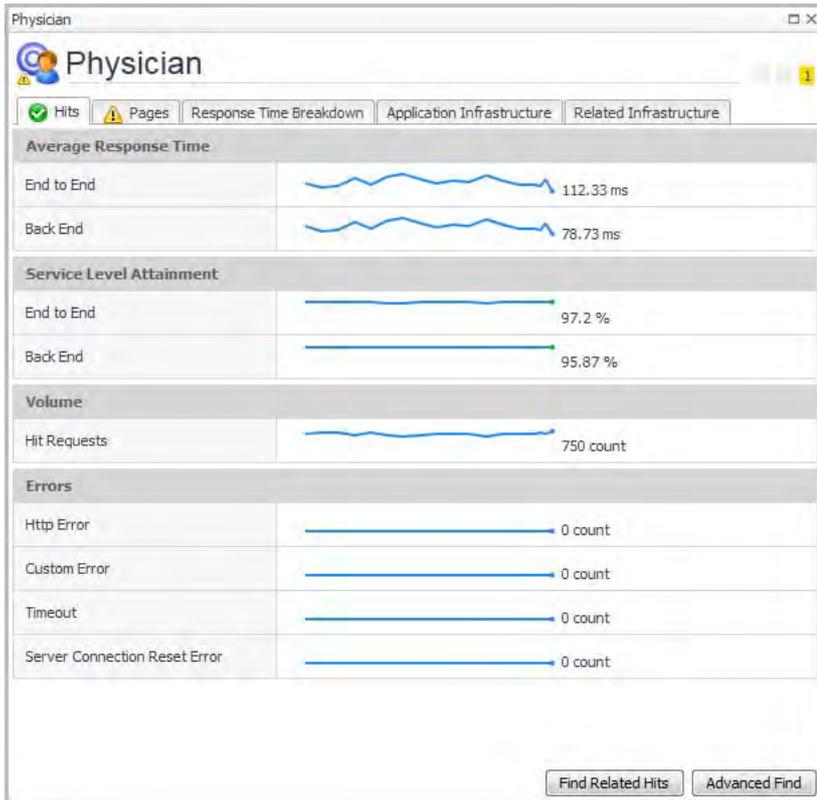
To investigate a transaction:

- 1 On the navigation panel, under Dashboards, click **APM > Transactions**.
- 2 Click the down arrow in the **Show transactions in** box and select the transaction group you want to view from the list.
- ① **TIP:** Use the Tile Display Options, located in the action panel on the right, to control how many tiles are displayed and how data is rolled up for viewing. For more information, see [Configuring display options](#).
- 3 Locate a transaction group that is experiencing errors. For example, users in the *Physician* transaction group are experiencing poor performance. The health status icon indicates Warning status . The transaction has not yet experienced a complete failure, but some component needs attention.

Figure 3. A transaction group, with the warning status illustrated



- 4 Click the name of the transaction in the title bar of the tile to drill down for more information. The transaction detail view opens.

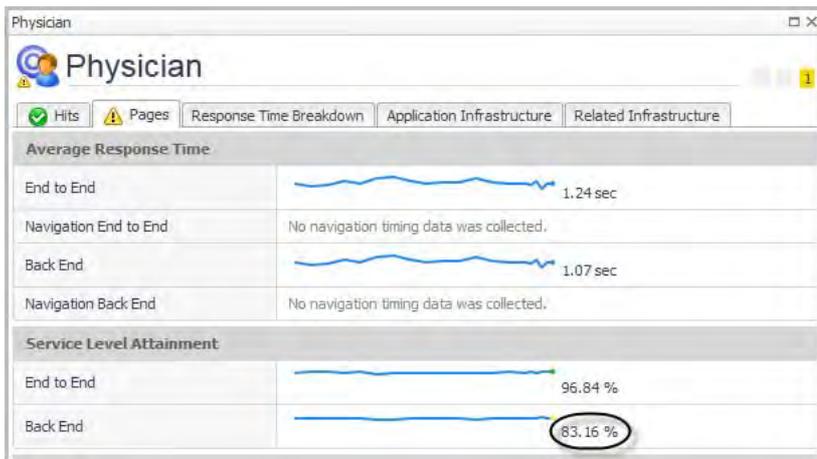


TIP: The detail view, and the tabs available, depend on the type of transaction selected. For example, drilling down on a [Real User \(APM\) tile](#) opens a performance detail view (as shown), while drilling down on a pivot result opens a summary view with tiles for each type of pivot you have defined (see [Pivot Breakdown detail view](#) for details).

The Hits tab and Pages tab summarize the pivots available from the hit analyzers configured for the transaction.

- 5 Click the Pages tab. Here you can see that the Warning status has been triggered by the Service Level Attainment for Back End dropping below an acceptable threshold.

Figure 4. An example of the Pages tab of a transaction detail view



- 6 Click Find Related Hits to investigate further.

The Search Hits page opens. From here, you can continue your investigation using the Search dashboards.

NOTE: The execution times in this view are aggregated for the current timeslice.

For more information about the tiles, detail views, and metrics, see [APM tile and view reference](#).

Investigating application server transactions

The Transactions dashboard allows you to visualize application-specific transaction data (that is, Java™ EE or .NET® transactions) with or without end user data. Use this dashboard to quickly identify if any transactions are having issues, and to view preliminary information that can aid in troubleshooting, including geographic discrepancies and whether the performance problems are in the back-end architecture, or the client-side browser or network.

TIP: The Service Operations Console includes a Transaction tab that displays transactions as services. The investigative workflow is similar to that described here.

In order to populate the Transactions dashboard or the SOC Transactions tab with data from Foglight for Java EE Technologies or Foglight for Microsoft .NET (version 5.9.1 or later), ensure that you used the appropriate procedures.

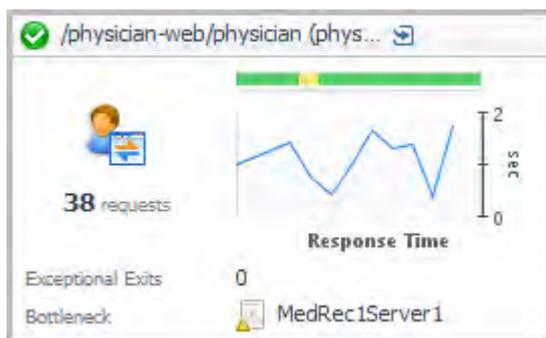
To investigate an application server transaction:

- 1 On the navigation panel, under Dashboards, click **APM > Transactions**.
- 2 Click the down arrow in the **Show transactions in** box and select the transaction group you want to view from the list.

TIP: Use the Tile Display Options, located in the action panel on the right, to control how many tiles are displayed and how data is rolled up for viewing. For more information, see [Configuring display options](#).

- 3 Locate an application server transaction group.

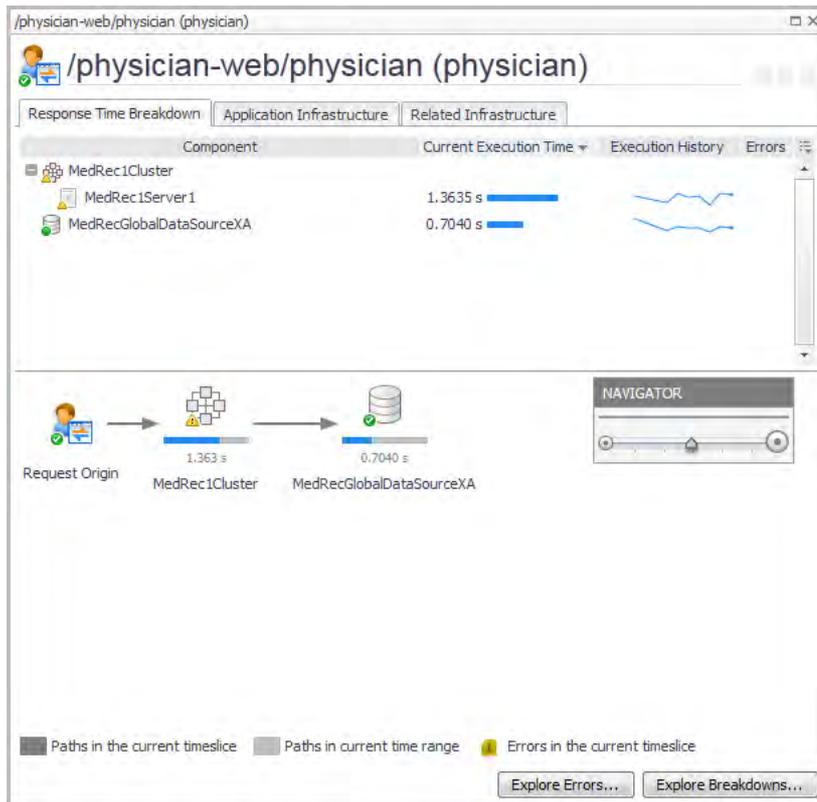
Figure 5. An example of a bottleneck appearing on a transaction group tile



In this example, `MedRec1Server1` is causing a bottleneck. It is performing poorly, as indicated by the warning icon ().

- 4 Click the name of the transaction (`/physician-web/physician (phys...)`) in the title bar of the tile to drill down for more information.

The transaction detail view opens.



5 On the Response Time Breakdown tab you can see the execution time for a request as it passes through the various components that are included in the transaction group.

NOTE: The execution times in this view are aggregated for the current timeslice.

- The upper portion of the tab provides a list of components, with average execution times for the current timeslice, and a sparkline that illustrates the average execution time during the selected time range.
- The lower portion of the tab provides the same average execution time information in a dependency path view. The average execution time for each component is displayed below the icon for the component.
- Application servers are clustered in the dependency view. The list of components provides a tree view of servers included in the cluster.
- The dark grey arrows (*Paths in the current timeslice*) indicate the path taken by at least one request in the current timeslice (that is, the most recent sample period reported by the agent).
- The light grey arrows (*Paths in current time range*) indicate the path taken by at least one request in the time range selected with the zonar (for example, the last four hours).
- A yellow exclamation mark indicates that an error has occurred within the marked component during the current timeslice.

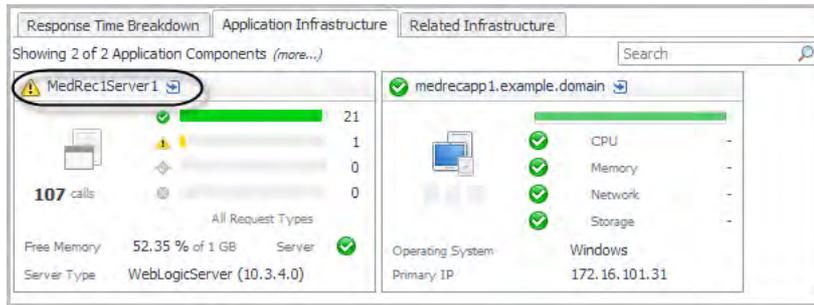
Here you can see that the execution time for the application server MedRec1Server1 is longer than it should be to meet service levels.

6 From here you can:

- Click **Explore Breakdowns** to open the Response Time Breakdown Explorer.
- Click **Explore Errors** to open the Error Breakdown Explorer.
- Click the **Application Infrastructure** tab to investigate the application components. This tab displays a tile for each component. In this example, there is a host (*medrecapp1.example.domain*) and an application server (*MedRec1Server1*).

Here you can see that the application server has a warning related to one request.

Figure 6. Application server with a warning related to one request



- 7 Click the name of the application component in the title bar of the tile to drill down for more information.

For example, click *medrecapp1.example.domain* to investigate the host performance in the [Host detail view](#). Or click *MedRec1Server1* to investigate the requests in the [Application Server detail view](#).

For more information about the tiles, detail views, and metrics, see [APM tile and view reference](#).

Configuring display options

You can customize the layout of the **Transactions** dashboard by selecting the appropriate options in the **Tile Display Options** dialog box. Use these options to control the total number of tiles, the order in which they appear, and the rollup options for multiple FTR locations (if applicable).

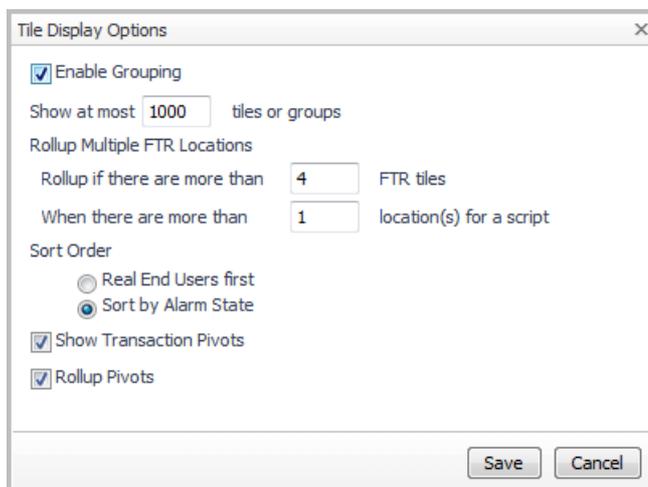
 **NOTE:** These settings apply on a per-user basis.

To configure display options:

- 1 With the **APM > Transactions** dashboard open in the display area, open the action panel on the right side of the browser interface.
- 2 Click **Tile Display Options**.

The **Tile Display Options** dialog box opens.

Figure 7. **Tile Display Options** dialog box



- 3 Configure the following options, as required.

- The **Enable Grouping** option groups user tiles together by transaction name. By default, groups are sorted by their severity first, then by their name. This grouping is not affected by the Sort Order options.
- The **Show at most n tiles or groups** setting determines the total number of tiles displayed. Synthetic transaction locations are first rolled up using the rollup criteria below. After that, the total number of tiles is determined by the maximum number of tiles that you specify.
- You can roll up synthetic transactions locations into multi-location FTR (Synthetics) tiles based on the criteria below, in the following order:
 - the maximum number of single-location Synthetics tiles, using the **Rollup if there are more than n FTR tiles** setting, and then
 - the maximum number of locations per script, using the **When there are more than n location(s) for a script** setting.
- Use the **Sort Order** options to sort the tiles by either type (**Real End Users first**) or alarm severity (**Sort by Alarm State**).
- For example, you can configure the **Transactions** tab to display a maximum of ten tiles sorted by the alarm state (highest severity first).
- The **Show Transaction Pivots** option controls whether transaction pivots are displayed. If you do not want to see [Pivot tiles](#), clear this check box.
- The **Rollup Pivots** option controls whether pivot data are grouped together or rendered individually. For example, Foglight can roll up all pivots such as Chrome™, Firefox®, Internet Explorer®, and Opera™ into a single web browsers pivot tile.

4 Click Save.

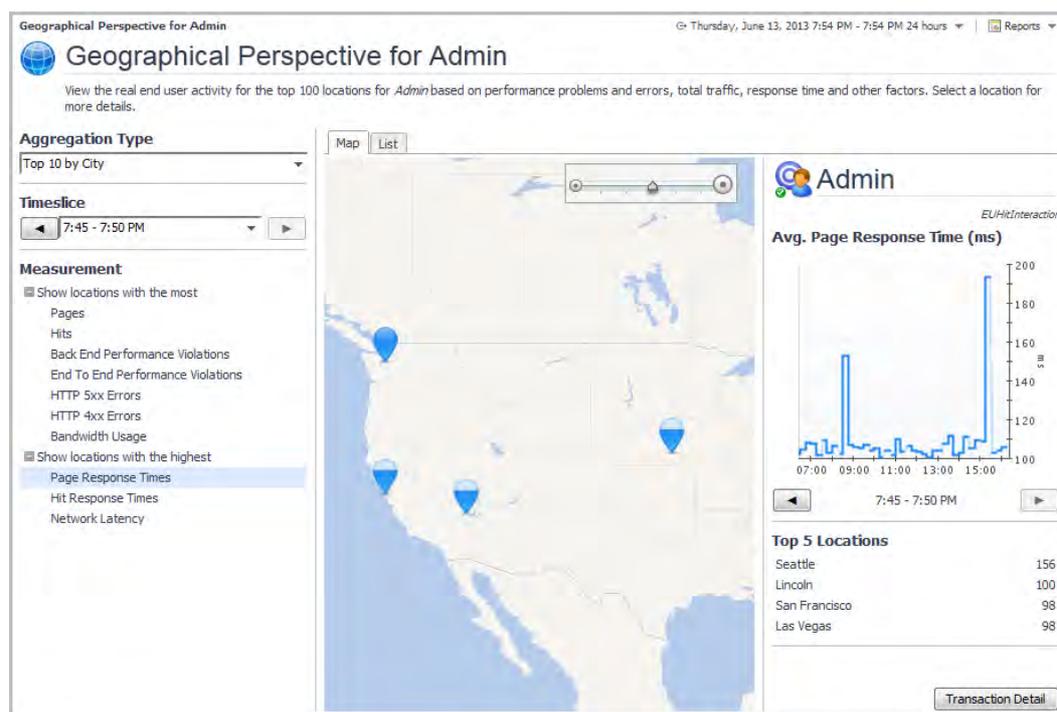
The Tile Display Options dialog box closes and the Transactions dashboard refreshes, reflecting the updated display options.

Viewing real user activity from a geographical perspective

The Geographical Perspective dashboard displays the real user activity for a selected transaction based on performance problems and errors, total traffic, response time, and other factors. The default view provides a summary for the top 100 locations for the selected transaction. A list of performance-related measurements (such as, “Show locations with the most: Hits” or “Show locations with the highest: Hit Response Times”) help you find performance patterns and problems with geographical features.

- NOTE:** If the Geographical Perspectives dashboard shows the message “There is no data to display,” an APM Administrator needs to update hit analyzers to populate the map with data. For more information, see “Publishing hit metrics for use in the Geographical Perspective dashboard” in the *Foglight APM Administration and Configuration Guide*.

Figure 8. Geographical Perspective for Admin dashboard



The Geographical Perspective dashboard is divided into three panes. The pane on the left contains lists of: available aggregation types, timeslices, and measurements. The center pane displays either a map, if the *Map* tab is selected, or a list of results in a tabular format, if the *List* tab is selected. The pane on the right provides graphical results from the measurements, and the option to drill down for more information.

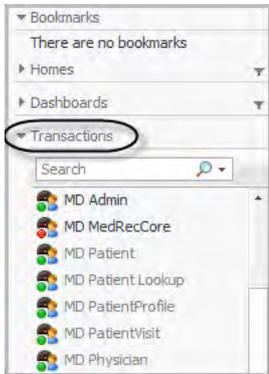
- NOTE:** If you are using a version 5.6.4 Management Server, only the List tab is available. The Map tab requires Management Server 5.6.5 or later.

If you are using Internet Explorer® (IE) 8 or earlier, only the List tab is available.

To view real end user activity in a geographical perspective:

- 1 On the navigation panel, under Dashboards, click APM > Geographical Perspective.
- 2 Select a transaction from the Transactions list at the bottom of the navigation panel.

Figure 9. Navigation panel showing a list of Transactions

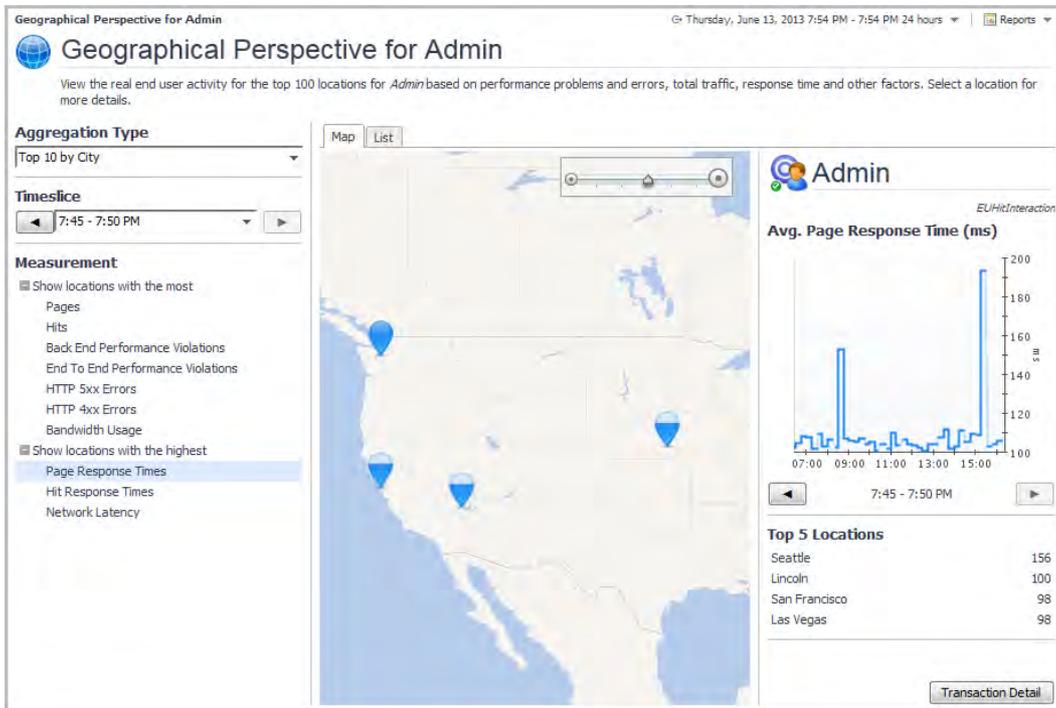


The dashboard display updates.

- 3 On the left side of the dashboard, select an **Aggregation Type**: top ten by city, country, or region.
- 4 Select a **Measurement** from the list to view the related transaction data. The map and right pane update based on your selection.

For example: select **Show locations with the highest: Page Response Times**.

Figure 10. Showing locations with the highest: Page Response Times



The map updates to indicate the locations that are experiencing the highest average page response times in the selected timeslice. The right pane displays a chart of the page processing time for the entire transaction (all locations), and the top five locations are listed in a table below the graph and timeslice selector.

Double-click anywhere on the map to zoom in on that location. You can also use the zoom tool in the map pane to zoom in or out. You can move the map in any direction by clicking and holding the left mouse button and dragging the cursor.

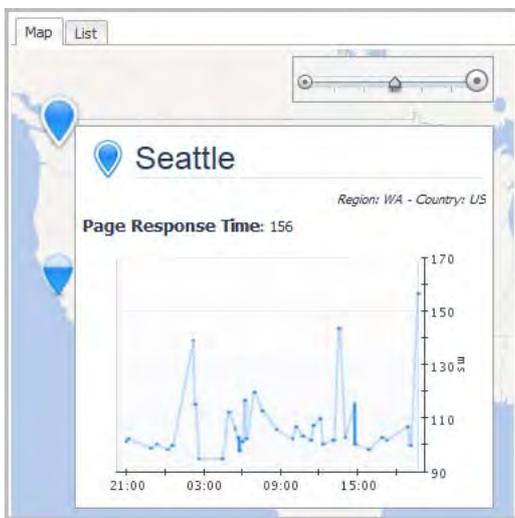
The fill-level of each pin on the map shows how close that location is to the maximum value in the current timeslice. In this example, Seattle has the highest response time, so its pin appears full.

- 5 Select a timeslice from the Timeslice list, or use the forward or back arrows to step through the available timeslices.

 **TIP:** The vertical blue bar on the graph indicates the currently selected timeslice.

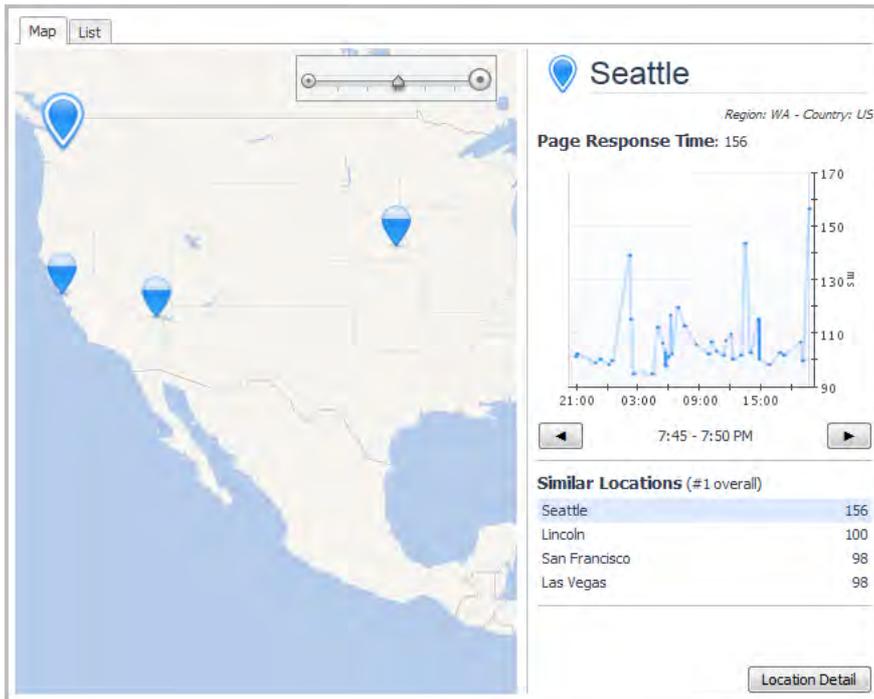
- 6 Click **Transaction Detail** (in the lower right corner of the right pane) to open the Summary view for the transaction. For more information about this view, see [Real User \(APM\) Performance detail view](#).
- 7 Hover your cursor over a pin to open a quick view of metrics for that location.

Figure 11. Metrics for a selected location



- 8 Click a pin to view a graph of the average page response time for that location in the right pane.

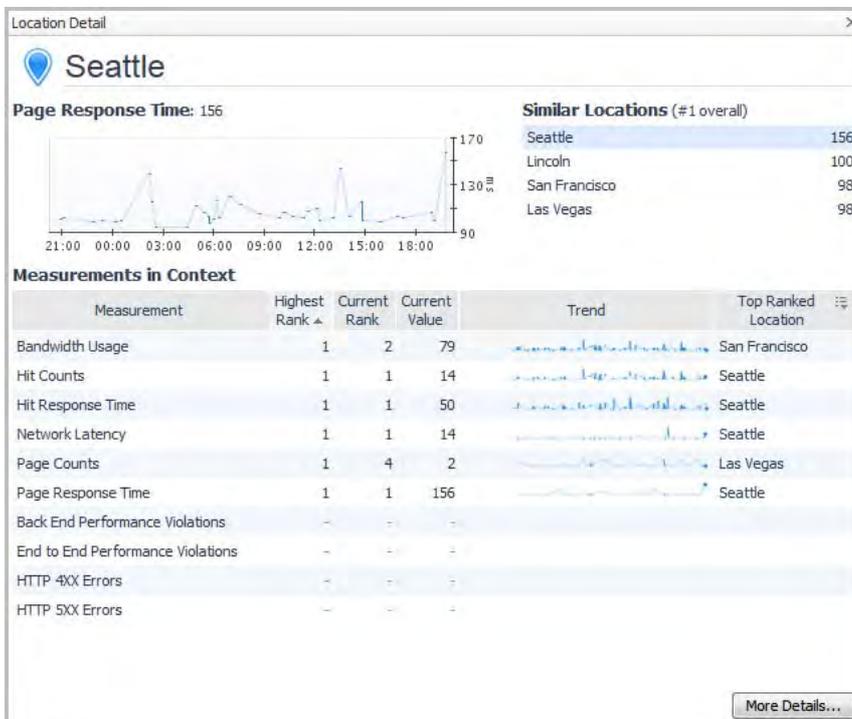
Figure 12. Select a city to see its response times



The Similar Locations list, in the right pane, updates to show locations that are ranked near the selected location in the current category. These are locations that have similar performance measurements to the selected location. Click any location name in the list to view the graph for that location.

- 9 Click Location Detail to drill down to detailed information for the selected location.

Figure 13. Detailed information for a selected location



The Location Detail view provides a table of measurements in context that helps you understand how the selected location is behaving relative to other locations during the selected timeslice and aggregation period.

Measurements for the selected location are sorted in order of severity.

The value in the Highest Rank column indicates the highest ranking that the selected location attained at any point during the selected time range. The time range may span multiple timeslices. For example, at some time during the selected time range, Seattle had the highest page response time of all locations. Therefore, for the measurement Page Response Time, Seattle's Highest Rank is 1 (first).

The value in the Current Rank column indicates the selected location's current ranking for the selected timeslice. This may or may not be the same as its highest rank, depending on when the peak value for the location occurred. In this example, Seattle is ranked second for the Current Rank for Bandwidth Usage. That is, during the currently selected timeslice, Seattle has the second highest page response time.

10 Click any location's name in either the Similar Locations list or the Top Ranked Location column to open a detail view for that location for comparison.

11 To view the transaction data for the selected location in the appliance, click **More Details**.

The **Search Hits** page opens. From here, you can continue your investigation using the Search dashboards.

Assessing real user experiences during key sequences

Sequences enable you to assess the experiences of your real users as they navigate a series of predefined steps within your web site or application. Using the aggregated data in the tiles on the Sequence Explorer dashboard, you can identify trends in how users navigated a selected sequence.

NOTE: APM Administrators define the sequences that appear in the Sequence Explorer. For more information, see “Introducing sequence analyzers” in the *Foglight APM Administration and Configuration Guide*.

You can use sequences for the following kinds of situations:

- For a commercial web application, a shopping sequence may reveal that fewer shoppers than expected purchased the objects in their shopping cart. By drilling down on the tile with the most exits, you can analyze the hits that occurred within the sequence. You may find that shoppers became frustrated with the time it took for the checkout page to load.
- For an intranet timesheet application, a timesheet update sequence may show that a significant number of employees abandoned an update at the same step. On further investigation, you may find that the affected employees received error pages.
- Part of developing web sites and applications includes identifying the critical paths within the application and optimizing the performance of those workflows. You can use sequences to monitor performance of those workflows over time and alert when problems arise.

You can perform the following tasks:

- [Introducing the Sequence Explorer dashboard](#)
- [Investigating sequence activity](#)
- [Changing the timeslice and the time range](#)
- [Creating custom Sequence Explorer dashboards](#)

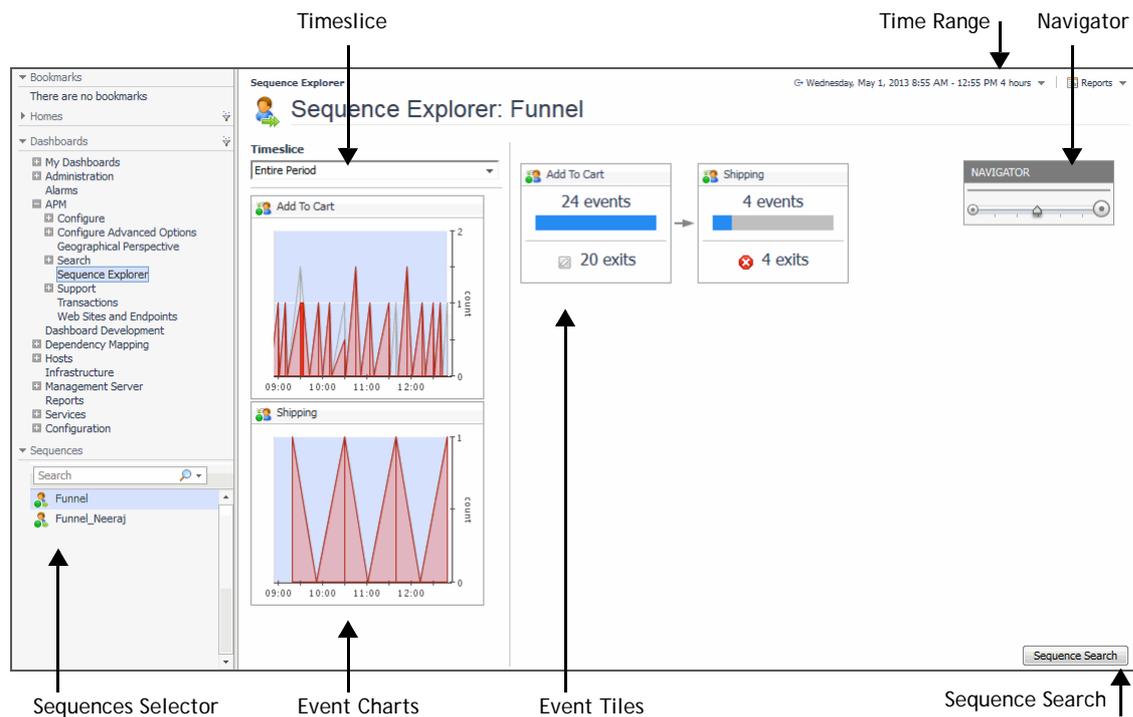
Introducing the Sequence Explorer dashboard

In the Sequence Explorer dashboard, you can explore the aggregated data for all events in a sequence and identify trends in how users navigated the sequence.

To open this dashboard:

- On the navigation panel, under Dashboards, click **APM > Sequence Explorer**.
The Sequence Explorer dashboard appears, displaying the Entire Period Timeslice details (by default) for a sequence that reflects a key workflow in your web site or application.

Figure 14. Sequence Explorer dashboard



The dashboard contains the following components.

Table 3. Sequence Explorer dashboard components

Component	Description
Sequences Selector	Select the sequence that you want to explore.
Timeslice	Select a timeslice to review. To view more timeslice intervals, increase the time range. To see previous timeslice intervals, move the time range to that particular time. For more information, see Changing the timeslice and the time range
Time Range	Controls the period of time represented in the dashboard. The default is the last four hours.
Event Charts	Displays the number of users in the event over the selected Time Range . The stacked area chart identifies the number of users who exited the sequence (top) and the number of users who remained (bottom) at each data point. To identify timeslices of interest, use the charts to look for spikes representing a high number of exits compared to the number of entries into the event. Then you can select the timeslice from the Timeslice list, and display data from that period in the event tiles.
Event Tiles	Displays the number of users in the event during the selected Timeslice . The tile states the number of users who started the event and the number of users who exited the event during the timeslice. The blue bar on the tile represents the percentage of users who are still engaged in the sequence at the beginning of this event.
Navigator	Zoom in on the event tiles displayed on the dashboard. To enlarge or reduce the size of the tiles, click and drag the arrow to the left or right on the gauge. To position this tool, click and drag it into a new location.
Sequence Search	View the list of sessions during which users navigated the defined sequence. The aggregated values shown in the Sequence Explorer are based on these sequence attempts. For more information about the Search Sequences dashboard, see Searching and investigating sequences .

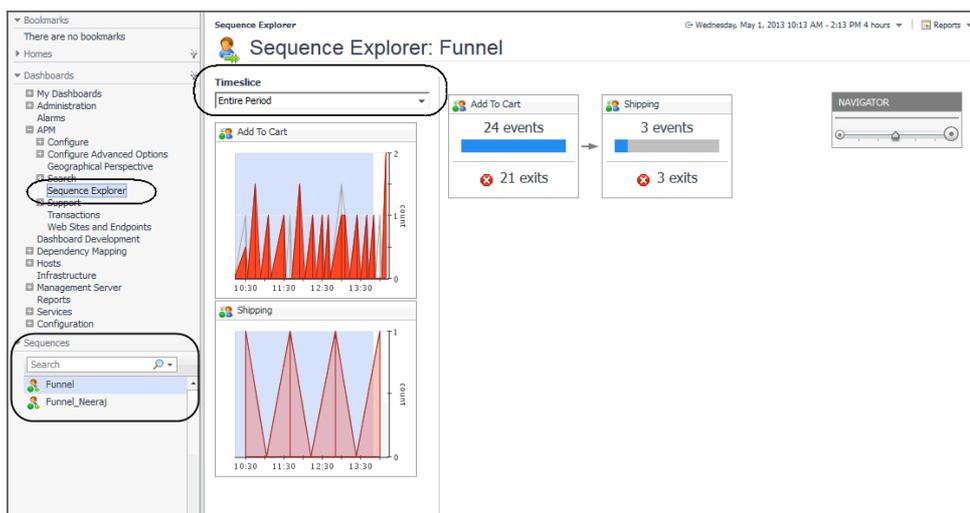
Investigating sequence activity

The following workflow describes how to select a sequence to display in the Sequences Explorer and suggests one way of identifying events that warrant further investigation.

To explore sequences:

- 1 On the navigation panel, under Dashboards, click **APM > Sequence Explorer**.

The Sequence Explorer dashboard opens, displaying content for the entire period of the time line available (default Timeslice).



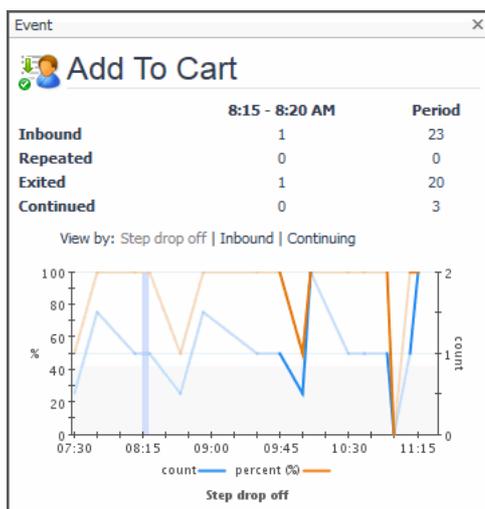
- 2 On the navigation panel, under Sequences (same level as Dashboards), select a sequence from the list or use the search field to find and select a named sequence.

The selected sequence appears. The data in the dashboard represents the entire time range. You can focus on a slice of time within the time range by selecting a time from the Timeslice list. For more information, see [Changing the timeslice and the time range](#).

- 3 To investigate why users exit the sequence at an event, click an event tile with a high number of exits.

The Event tile dialog box opens, displaying top-level details for the target sequence events.

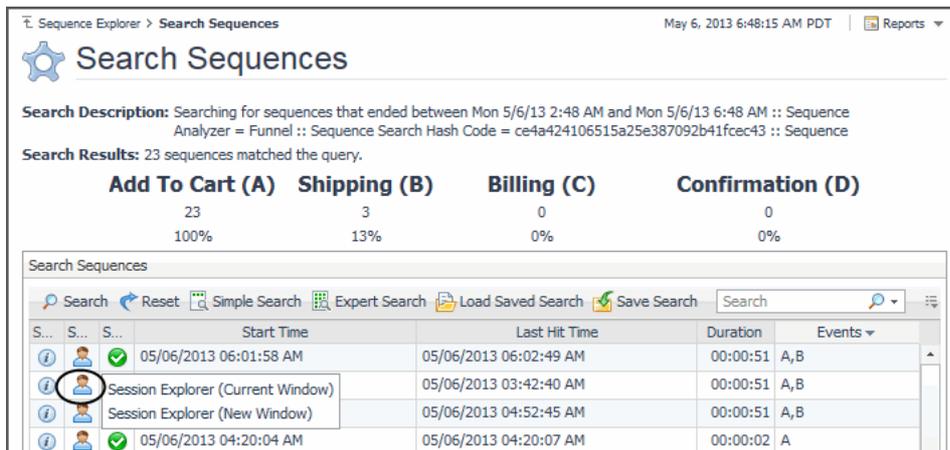
Figure 15. Event Tile dialog box



For more information about the information presented in this dialog box, see [Investigating Event tiles details](#).

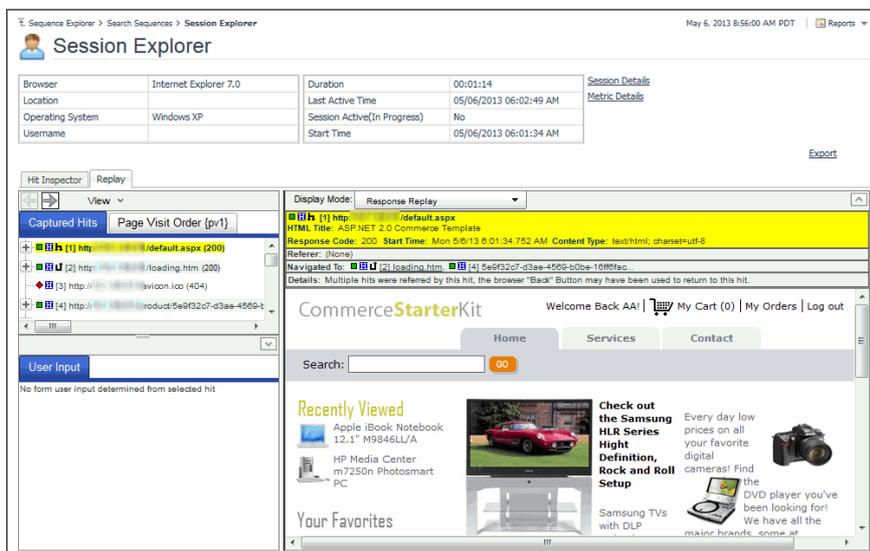
- 4 To evaluate individual user experiences, navigate to the expanded details in a Search Sequences dashboard.
 - a On the Event tile dialog box, click a number to display the filtered Search Sequences results. In the proceeding example image, clicking 20 (in the row under the Period) displays the 20 sequences during which users exited the sequence at this event. For information about search results, see [Understanding search sequences results](#).

Figure 16. Search Sequences dashboard



- b In the Search Sequences dashboard, select a sequence to investigate and click its Session Explorer icon. The Session Explorer opens to display the captured hits, page visit order, and other details. For more information, see [Replaying sessions, hits, and sequences](#).

Figure 17. Session Explorer dashboard



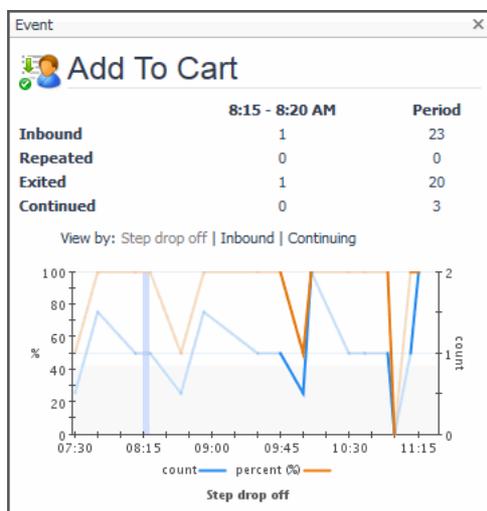
- c To return to the Sequence Explorer dashboard, click Sequence Explorer in the breadcrumb trail at of the display area.

For additional information, see [Investigating Event tiles details](#).

Investigating Event tiles details

Clicking an event tile displays additional information about the sequence event.

Figure 18. Event tile



The following values are displayed at the top of the dialog box.

Figure 19. Event tile dialog options

	8:15 - 8:20 AM	Period
Inbound	1	23
Repeated	0	0
Exited	1	20
Continued	0	3

Table 4. Event tile dialog box options

Option	Description
Inbound	Displays the number of hits coming into the event. For example, when a user buys a book online, the user first does a search and then adds it to the shopping cart. From the initial search to adding it to the shopping cart, counts as 1 inbound. The preceding image displays 1 inbound between the timeslice of 8:15 - 8:20 AM, meaning one user hit for this event during this specified timeslice. The Period value shows that 23 users were inbound for the entire specified time range (zonar).
Repeated	Displays the number of hits made in the same event. For example, if a user first does a search and that search takes a number of hits until the user finds the book they are looking for, the search event traces the number of times the user entered a search. The preceding image shows that no repeated searches occurred during the 8:15 - 8:20 AM timeslice (Repeated = 0). The Period value shows that no users repeated the same event during the entire specified time range (zonar).
Exited	Displays the number of hits where users exited without moving to a next event or repeating the same event. For example, if a user searches for a book and then closes the browser, this counts as 1 inbound and 1 exit. The preceding image shows that 1 user exited between 8:15 - 8:20 AM. The Period value shows a total of 20 users exited the event during the specified time range (zonar).
Continued	Displays the number of hits where users continued to move through the events. The preceding image shows that no users continued to move to another event during the timeslice 8:15 - 8:20 AM (Continued = 0). The Period value, however, shows that 3 users continued with the sequence during the specified time range (zonar).

At the bottom of this dialog box, you can select one of the following views.

Figure 20. Event tile “Select by” views

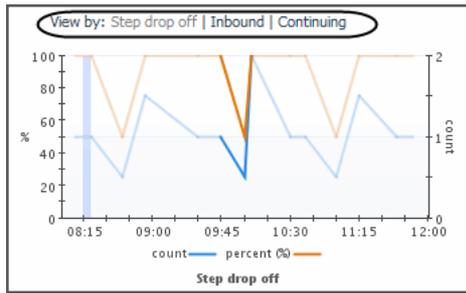


Table 5. Event tile “Select by” view options

Option	Description
Step drop off	Displays both the exit rate percentage and actual exit count for the event (% scale on the left axis and count scale on the right axis). This is the default view.
Inbound	Displays a detailed breakdown of hits initiated from a previous event in the sequence. The name of the inbound event and value is displayed. Click an event to display the details of the inbound event.
Continuing	Displays a detailed breakdown of hits continuing to a next event in the sequence. The name of the continuing event and value is displayed. Click an event to display the details of the continued event.

Changing the timeslice and the time range

By default, the Sequence Explorer shows details for the Entire Period Timeslice. You can change the time range (zonar) and select a different timeslice to focus your investigation.

Selecting a five minute timeslice enables you to review the activity during that time in the Event tiles. The Event tiles allow you to drill into time slices that had particularly high exits. In the example below, one user started an event and also exited that event during the 8:45 - 8:50 AM timeslice.

Figure 21. Changing the timeslice for the Sequence Explorer



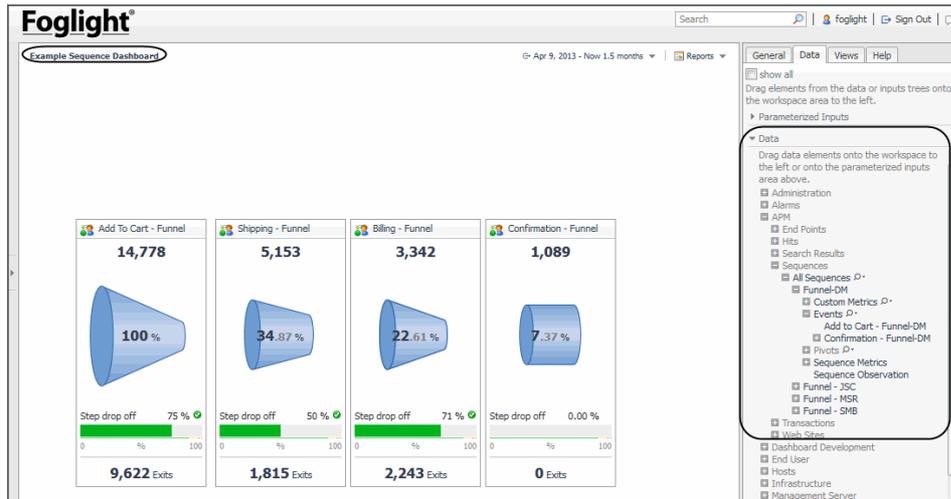
Changing the time range updates the information in the Event charts. By default, the time range is set to four hours. You can change the time range to represent a time period in the past, or to increase or decrease the range of the current time period. For example, if you are interested in locating a sequence that occurred in the previous week, set the time range to that time frame. For more information about using the time range (zonar), see the [Foglight User Help > Online-Only Topics > Zonar and Time Range topic](#).

Creating custom Sequence Explorer dashboards

In addition to using the Sequence Explorer dashboard, you can create custom sequence events dashboards for your specific needs. These dashboards can contain any combination of tables and charts that you find useful. The custom dashboards that you create are located under **My Dashboards** in the navigation panel.

In the following image, APM > Sequences > All Sequences > Funnel-DM > Events data elements are dragged from the Action panel Data tab and positioned on the display area, using the Sequence Event Funnel template.

Figure 22. Creating custom Sequence Explorer dashboards example



For more information, see [Creating custom drag-and-drop dashboards](#) or see the [Foglight User Help > Online-Only Topics > Creating a Custom Dashboard](#) topic.

TIP: Visit edocs.quest.com to watch our learning videos. See [How to create custom Foglight dashboards](#).

Monitoring the performance of web sites and endpoints

If a physical or virtual web server experiences issues, or if a web site or web application has performance issues such as memory leaks, then real users are likely to experience performance issues as well. Network administrators and application owners need to be able to assess the performance of web sites and applications in real time and through historical data.

For more information, see the following topics:

- [Introducing the Web Sites and Endpoints dashboard](#)
- [Exploring the top busiest web sites or endpoints](#)
- [Exploring alarms on web sites or endpoints](#)
- [Investigating a web site or endpoint](#)
- [Troubleshooting an excessive number of monitored web sites](#)

Introducing the Web Sites and Endpoints dashboard

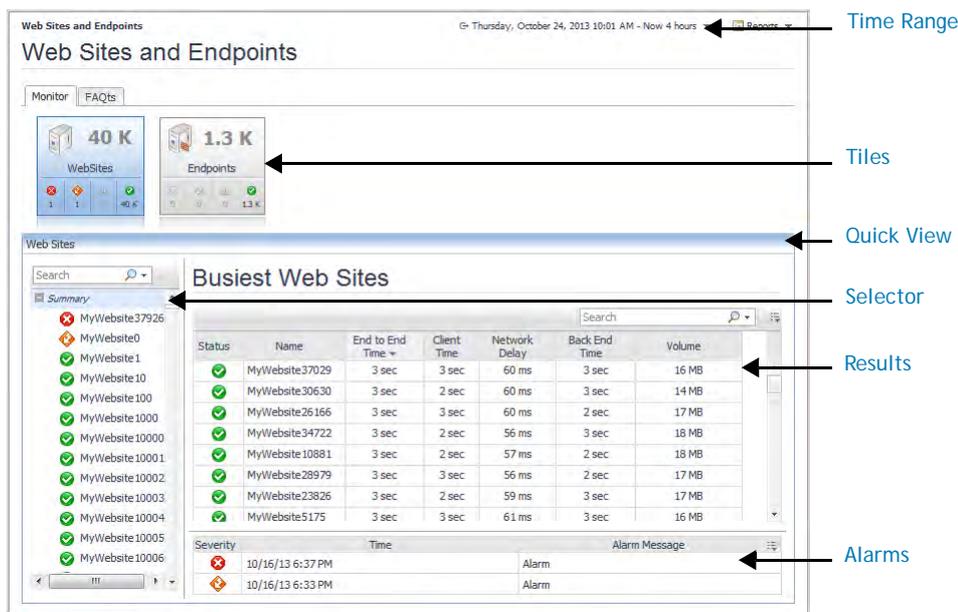
The Web Sites and Endpoints dashboard displays information about hit performance by web sites or by endpoints. Endpoints mark the termination or completion of a session or connection.

To open this dashboard:

- On the navigation panel, under Dashboards, click **APM > Web Sites and Endpoints**.

The first time you open this dashboard, the Busiest Web Sites view displays details about the top 50 busiest sites active in the period. The selector contains a list of all active sites.

Figure 23. Web Sites and Endpoints dashboard



The dashboard contains the following components:

Table 6. Web Sites and Endpoints dashboard components

Component	Description
Time Range	Controls the period of time represented in the dashboard. The default is the last four hours. For more information, search for "Time Range" in the online help.
Tiles	Summarizes how many Web Sites and Endpoints are being monitored, and breaks down the total number by alarm severity. Tiles control the Quick View area as follows: <ul style="list-style-type: none"> Click the top half of the Web Sites tile to open the Web Sites quick view with the Busiest Web Sites list displayed. Click the top half of the Endpoints tile to open the Endpoints quick view with the Busiest Endpoints list displayed. Click a severity icon in one of the tiles to open the matching quick view. The selector lists all sites endpoints with that alarm and the Busiest list contains the subset of sites endpoints with the alarm that are in the top 50.
Quick View	Contains three views: Selector, Results, and Alarms.
Selector	When the Web Site tile is selected, the selector lists sites and applications by name. When the Endpoints tile is selected, it lists endpoints as a combination of IP address and port number. The selector sets the Results view as follows: <ul style="list-style-type: none"> Click Summary to display the top 50 busiest sites endpoints. Click a site or endpoint to display charts for that site endpoint.
Results	Displays one of the following views: Busiest Web Sites, Busiest Endpoints, or performance charts for a selected site endpoint.
Alarms	Displays a list of the top 50 busiest sites endpoints that have alarms. Alarms are triggered when a site's or endpoint's performance matches a severity condition defined in a rule. For more information, search for "Alarms" and "Rules" in the online help.

Exploring the top busiest web sites or endpoints

The Busiest Web Site and Busiest Endpoint views are useful for understanding which of your monitored applications are busiest in terms of volume. Volume is the total size of all HTTP messages sent by both clients and servers, including content and headers for both requests and responses, during the time range. The views contain up to 50 of the busiest sites|endpoints active in the selected time range.

In addition to the Volume metric, the Busiest view contains the timing metrics used to measure hit performance: End-to-End Time, Client Time, Network Delay, or Back End Time. For a single hit, the End-to-End Time is the sum of the other three metrics. In this view however, the values represent average values for all hits over the time period. For more information about hit metrics, see the *Foglight APM Reference Guide*.

NOTE: Sorting the table by one of the timing metrics does not recalculate the top 50 sites|endpoints, it simply reorders the current results by the selected metric.

The following walkthrough assumes a scenario where all the top 50 sites are operating within expected parameters, that is, no alarms. For an approach to alarms, see [Exploring alarms on web sites or endpoints](#).

To explore the top busiest sites or endpoints:

- 1 In the navigation panel, under Dashboards, click **APM > Web Sites and Endpoints**.
The time range and selected tile are the same as the last time the dashboard was opened.
- 2 To show data for a different time period, set the [Time Range](#).
- 3 To change the quick view, click the top part of the desired tile.
In the quick view, the Selector displays a list of monitored sites|endpoints active in the time period, ordered first by severity and then alphabetically. The top-level node, *Summary*, is selected and the Busiest view shows up to 50 of the busiest sites|endpoints.
- 4 Sort the table by **Volume** to see the busiest sites|endpoints in terms of the total size of all HTTP messages sent and received.
- 5 Sort the table by **End-to-End Time** to see which of the busiest sites|endpoints also contributed to the longest average hit download times. Scan the values for the other timing metrics to determine where time is being spent: on the client side, traversing the network, or on the server side.
- 6 **Next Step:** [Investigating a web site or endpoint](#)

Exploring alarms on web sites or endpoints

When the performance of a monitored site or endpoint meets one of the conditions defined in a multiple-severity rule, Foglight triggers an alarm and sets the site's or endpoint's state icon to indicate the severity level of the performance issue. You should review any high-severity alarms that show up in the time range you are interested in.

TIP: You can modify the conditions in multiple-severity rules to better suit your environment. For more information, search for "Rules" in the online help.

The most important alarms to take action on are those that occur on a site or endpoint in the Busiest Web Sites or Busiest Endpoints views. The Alarm view highlights these sites|endpoints. In addition, any high severity (Fatal and Critical) alarms outside of the top 50 should be assessed. These alarms appear at the top of the selector list.

This walkthrough recommends setting the quick view and looking at the Alarm view to see if there are any alarms in the top 50 sites|endpoints. If you prefer to restrict the quick view to show one set of alarms, such as all Fatal alarms, start your investigation by clicking a severity icon on a tile.

To explore alarms in the *Busiest list*:

- 1 In the navigation panel, under Dashboards, click **APM > Web Sites and Endpoints**.
The time range and selected tile are the same as the last time the dashboard was opened.
- 2 To show data for a different time period, set the [Time Range](#).
- 3 Click the top half of the tile that has the highest number of sites|endpoints with the most severe errors.
The quick view updates. If there are any alarms in the top 50, they appear in the Alarm view.
- 4 In the Alarm view, assess all high-severity alarms.
 - a Start with the highest severity alarm in the list.
 - b Review the alarm details to understand the issue.
 - c Take action by resolving the issue yourself or by notifying the appropriate person.
 - d Repeat to resolve other alarms in order of severity.

 **TIP:** For Warnings, depending on the issue, an appropriate action may be to acknowledge the alarm and ignore it.
- 5 If the other tile shows alarms, select it and repeat step 4.
- 6 If you want, explore alarms that are not in the top 50.
 - a On a tile, click the state icon representing the worst severity.
The [Selector](#) displays all sites|endpoints with that alarm. The [Results](#) view shows the subset of the top 50 busiest sites|endpoints with that alarm (if any).
 - b In the selector list, select an alarm that was not in the top 50.
 - c Assess the alarm and take action as required.
- 7 **Next Step:** [Investigating a web site or endpoint](#)

Investigating a web site or endpoint

When you need more information than the *Busiest* view or *Alarm* view provides, select the site or endpoint of interest. The *Results* view changes to show a set of charts containing hit performance, page performance, warnings, and errors for the time range. You can use these charts to discover whether the average times reflects a consistent level of performance, or if the performance is uneven. From here, even more data is available by clicking a chart or the *Explore* button.

Many things can cause a sudden change in performance or errors. Here are a few possibilities:

- A page is deleted but there are still references to it, causing page errors.
- Changes to an application's code causes slower responses to hit requests.
- An ISP is experiencing higher than normal volume resulting in higher client times.
- Web servers are temporarily down in a server farm, and the remaining servers are overloaded.
- A change occurs in the infrastructure, such as a vMotion[®] that moves an application to a less responsive host.

 **NOTE:** For descriptions of the metrics in this and other dashboards, search the online help using the metric name. For hit errors and warnings, look up "Status Metrics."

To investigate a web site:

- 1 Click a site|endpoint.
Charts reflect performance for the time period.

Table 7. Investigating a web site or endpoint

View	Description
Page Performance	For pages, displays time spent on the server side, the network, and the client side.
Hit Performance	For hits, displays time spent on the server side, the network, and the client side.
Errors	Displays errors on hits that occur during the time range.
Warnings	Displays warnings on hits that occur during the time range.
Alarms	Displays alarms for this site endpoint, if any.

- 2 Look for clues to issues, such as:
 - A sudden change in performance over the time range.
 - An onset of warnings and errors where none existed in previous time ranges.
 - Consistently higher than expected values for one of the metrics.
- 3 If you need more details to understand the issue, click **Explore**.
A dashboard opens for the selected site|endpoint.
- 4 Review overall performance in the **Summary** tab. The Summary tab is similar to the preceding view, but adds the following metrics for the time period: End to End Time, Capture Rate, and Volume.
- 5 To investigate hit performance, click the **Hits** tab. The Hits tab displays detailed hit performance and hit volume metrics plus request and response code metrics for the time period.

Table 8. Hits tab views

Views	Purpose
Hit Performance	Displays metrics that contribute to overall hit performance. This chart includes the initial response time.
Hit Volume	Displays metrics that contribute to the overall hit volume, including the size of headers and content for both requests and responses.
HTTP	Displays the request methods and response codes issued for hits on this site endpoint.
Warnings and Errors	Displays warnings and errors for the hits associated with this site endpoint.
Alarms	Displays alarms for this site endpoint, if any.

- 6 To investigate page performance, click the **Page** tab. The Page tab displays detailed page performance and page volume metrics for the time period.

Table 9. Page tab views

Views	Purpose
Page Performance	Displays additional metrics that contribute to overall page performance, including redirects and incomplete downloads.
Page Volume	Displays additional metrics that contribute to the overall page volume, including the size of headers and content for both requests and responses.
Warnings and Errors	Displays warnings and errors for the pages associated with this site endpoint.
Alarms	Displays alarms for this site endpoint, if any.

- 7 To return to the previous dashboard, click **Web Sites and Endpoints** in the breadcrumb trail.

Troubleshooting an excessive number of monitored web sites

If you have an excessive number of web sites reported in this dashboard, consider aggregating data capture for similar sites. For example, if you attribute the data collected for alias sites to the primary site, then only the primary site appears in this dashboard. In general, data aggregation makes the data more manageable and more meaningful in all dashboards.

To define data aggregations, an APM Administrator creates domain rules. In a troubleshooting scenario, where you want a quick way to aggregate data for a large number of similar sites, use a regular expression that matches multiple sites and map the sites to a fictitious (or real) domain name. For information about defining domain rules, see “Managing domain rules” in the *Foglight APM Administration and Configuration Guide*.

 | **NOTE:** Only data captured after the domain rule is created is aggregated. Historical data is not affected.

Example

Consider a scenario where all sites of interest are identified in the dashboard by domain names, but Foglight APM is also monitoring a proliferation of IP addresses that are of little or no interest. The following regular expression matches all IP addresses and aggregates them under a single fictitious domain called *myOtherSites.com*. This rule eliminates the “noise” generated by all the extraneous sites and allows you to focus on what really interests you.

Find: `\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b`

Replace: `myOtherSites.com`

Searching APM data

Foglight captures, decrypts, analyzes, and stores a vast amount of data about how real users navigate your web sites and applications, the performance of the web servers and application servers in your infrastructure, and the performance of Java™ applications and .NET® applications. This data is stored as details in the Archiver database.

You can see the details when you drill down from the top-level dashboards (Geographical Perspectives, Sequence Explorer, and Web Sites and Endpoints dashboards). In the top-level dashboards, you view aggregated metrics derived from the details. For example, in the Sequence Explorer, you see exit counts that represent a total for all users who performed the same sequence of steps. When you drill-down on a tile, you can navigate to the expanded details in a Search dashboard. So for the sequence, you can drill down to the captured sequences to evaluate individual user experiences.

You may come across situations where you want to search the Archiver database directly using your own search criteria. For example, if a real user reports having issues with your web site, you can search for the session and replay it to see what your user experienced. Each type of search has its own dashboard and offers a simple search and an expert search. You can save searches and rerun them later. You can also run the last search and clear search results.

From search results, you can replay a hit, sequence, or session to see what your real user experienced while navigating your site or application. You can also view search results in a map or pivot chart. For more information, see [Replaying sessions, hits, and sequences](#) and [Visualizing search results](#).

You can perform the following tasks from the Search dashboards:

- [Searching and investigating hits](#)
- [Searching and investigating sessions](#)
- [Searching and investigating sequences](#)
- [Viewing search results in a map](#)
- [Viewing search results in pivot charts](#)
- [Replaying sessions, hits, and sequences](#)
- [Repeating the last search](#)
- [Saving searches](#)
- [Running saved searches](#)
- [Clearing search results](#)

Searching and investigating hits

You can search for hits by time range, hit detail, analyzer, content category, or some combination of these parameters. You can also define match conditions to create very specific searches.

In the Search Hits dashboard, you can run a simple search or an expert search to find hits. You can also rerun the last search, save a search, load and run a saved search, or clear search results.

For more information, see the following topics:

- [Defining simple searches for hits](#)
- [Defining expert searches for hits](#)

- [Understanding search hits results](#)
- [Investigating hit results](#)
- [Viewing search results in a map](#)
- [Viewing search results in pivot charts](#)
- [Replaying sessions, hits, and sequences](#)
- [Repeating the last search](#)
- [Saving searches](#)
- [Running saved searches](#)
- [Clearing search results](#)
- [Defining match conditions for expert searches](#)

Defining simple searches for hits

A simple search enables you to search for hits using the most commonly-used search criteria. If you want to search for hits that occurred within a particular time range or hits that match some set of conditions, you need to define an expert search instead.

To define and run a simple hit search:

- 1 In the navigation panel, under Dashboards, click **APM > Search > Hits**.
- 2 Click **Simple Search**.
- 3 Specify the search criteria.

Table 10. Simple hit search criteria

occurred within the	Select the time range for the search. If no other options are set, the search returns all hits occurring within the specified time range. TIP: An APM Administrator can increase or decrease the maximum time range displayed in the list through the Configure Advanced Options > Settings dashboard. See the <i>Search Time Range Limit</i> option under the Archiver Query Settings.
Hit Analyzer	Optional—search by hit analyzer name. Specify the name of the hit analyzer that captures the data you want to find.
Request Path	Optional—search hits based on the URI path. Specify a full or partial path using asterisks (*) as wildcards as required. For example, <i>/css*</i> returns all hits that have the subdirectory <i>css</i> in the Request Path hit detail.
Content Category	Optional—search for hits in a particular content category. Select a content category from the list.
Violates the	Optional—search for hits that caused a specified threshold to be exceeded. Select a threshold from the list.

- 4 Click **Search**.

The Search Hits table contains the results of the search.

Defining expert searches for hits

You can run a search using the same options as a simple search. You can also define a time range or some set of conditions.

To define and run an expert hit search:

- 1 In the navigation panel, under Dashboards, click **APM > Search > Hits**.
- 2 Click **Expert Search**.

If you defined a simple search before switching to an expert search, the Expert Search dialog box displays the same values for the options you selected in the Simple Search dialog box.

- 3 Specify the search criteria.

Table 11. Expert hit search criteria

Time Range	Select the time range for the search. If no other options are set, the search returns all hits occurring within the specified time range. TIP: An APM Administrator can increase or decrease the maximum time range displayed in the list through the Configure Advanced Options > Settings dashboard. See the <i>Search Time Range Limit</i> option under the Archiver Query Settings.
starting	If you selected <i>Time Range=specified time range</i> , click the Calendar  icon and specify a date and time.
ending	If you selected <i>Time Range=specified time range</i> , select a length of time to search (starting from the <i>starting</i> time).
Hit Analyzer	Optional—search by hit analyzer name. Specify the name of the hit analyzer that captures the data you want to find.
Response Content	Optional—search by keyword. Specify a keyword that you want to match in the Response Content hit detail.
Request Path	Optional—search hits based on the URI path. Specify a full or partial path using asterisks (*) as wildcards as required. For example, <i>/css*</i> returns all hits that have the subdirectory <i>css</i> in the Request Path hit detail.
Content Category	Optional—search for hits in a particular content category. Select a content category from the list.
Match Conditions	Optional—specify one or more conditions to match. Click Add . You can define a match condition on any hit detail or metric listed in the Source list. For help creating match conditions, see Defining match conditions for expert searches .

- 4 Click **Search**.

The Search Hits table contains the results of the search.

Understanding search hits results

When the search ends, the results are displayed in the Search Hits table. The search parameters appear above the table. If no hits matched the search parameters, the table is empty.

-  **TIP:** By default, a hit search returns a maximum of 1,000 hits. An APM Administrator can change this limit using the *Hit Search Result Limit* setting in the Configure Advanced Options > Settings dashboard.

Figure 24. Search Hits dashboard

The screenshot shows the Search Hits dashboard with a table of search results. The table has the following columns: Sessions, Status, Category, Hit End to End Time (ms), Hit Back End Time (ms), Page End to End Time (ms), Page Back End Time (ms), Navigation Page Completion Time (ms), Navigation Content Delivery Time (ms), URL, Client IP, Time, and Code. The table contains multiple rows of data, including hits for Image, HTML Fragment, and Style Sheet categories.

The Search Hits table may contain some or all of the following columns. To hide/show columns, click the Customizer icon (beside the Search field) and select the columns to show.

Table 12. Search Hits table

Column	Description
Sessions	When a hit belongs to a session, the Session Explorer and Session Detail View icons appear in this column. You can drill down to session details by clicking one of these icons.
Status	Indicates the hit status using the standard severity icons: <ul style="list-style-type: none"> Normal Warning Critical Fatal
Category	Identifies the content category for the hit.
Hits	Drill down to more detail about the hit by clicking Hit Detail View . View the content at the URL by clicking Replay Content Preview . Displays the custom fields updated by hit analyzers that matched a hit.
Custom Fields	NOTE: For a custom field to appear in search results, the custom field's Storage option must be set to <i>Show in search results</i> or <i>First column in search results</i> . See "Defining custom fields" in the online help.
HTML Title	When an HTML page includes an HTML title in its definition, displays the HTML title.
Hit End to End Time (ms)	Displays the time spent by the client-side browser and the web server on this hit, calculated using server timestamps. For more information, see "Tracking time spent on a hit" in the <i>Foglight APM Reference Guide</i> .
Hit Back End Time (ms)	Displays the total time spent by back-end servers processing HTTP requests sent from the client. For more information, see "Tracking time spent on a hit" and "Understanding what is included in Back End Time" in the <i>Foglight APM Reference Guide</i> .
Page End to End Time (ms)	Displays the total time taken to download a complete page, calculated using server timestamps. For more information, see "Tracking time spent on a page" in the <i>Foglight APM Reference Guide</i> .
Page Back End Time (ms)	Displays the sum of the Back-End Time values for all hits associated with the page.

Table 12. Search Hits table

Column	Description
Navigation Page Completion Time (ms)	Displays the total time taken from the beginning of a navigation action (such as a click on a hyperlink) to the end of the load event when the page has been completely displayed in the browser. For an example, see “Tracking time spent on a page using instrumentation” in the <i>Foglight APM Reference Guide</i> .
Navigation Content Delivery Time (ms)	Displays the time taken from the beginning of the request to the beginning of the response. For an example, see “Tracking time spent on a hit using instrumentation” in the <i>Foglight APM Reference Guide</i> .
URL	Displays the URL for each hit.
Client IP	Displays the client IP address of the real user.
Time	Displays the time the hit was initiated.
Code	Displays the HTML response status code for the hit.
Exception	Displays any exceptions that occurred while processing this hit.
Server IP	Displays the web server IP address.

Investigating hit results

This workflow walks through how to use the data in the Search Hits table and how to drill down to more details about a specific hit or the session to which it belongs. Your own investigative workflow will depend on the problems you are trying to resolve.

NOTE: Typically you want to design searches that limit the search results in a meaningful way, such as finding all hits that triggered a hit analyzer or all hits with an end-to-end time greater than 10 seconds. A restrictive search makes your investigation work much easier.

To review hit search results:

- From the Search Hits dashboard, run a search.
 - Running saved searches
 - Repeating the last search
 - Defining simple searches for hits
 - Defining expert searches for hits

For this walkthrough, we created a simple search with Content Category = HTML, and then sorted by Back-End Time (ms).

Figure 25. Search Hits dashboard (Content Category = HTML)

The screenshot shows the 'Search Hits' dashboard in Foglight. The search description is 'Searching for hits that occurred in the last 4 hours :: Content Category = HTML'. The search result shows 1000 hits in 390 sessions. The table below is a simplified version of the data shown in the screenshot.

Sessions	Status	Category	Hits	Hit End to End Time(ms)	Hit Rack End Time(ms)	Page End to End Time(ms)	Page Rack End Time(ms)	Navigation Page Completion Time(ms)	Navigation Content Delivery Time(ms)	URL	Client IP	Time	Code
1	✓	HTML	99	44	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:40 AM	200
1	✓	HTML	337	111	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:45 AM	200
1	✓	HTML	594	230	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:45 AM	200
1	✓	HTML	562	206	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:45 AM	200
1	✓	HTML	592	161	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:45 AM	200
1	✓	HTML	599	199	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:45 AM	200
1	✓	HTML	470	125	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:45 AM	200
1	✓	HTML	422	108	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:45 AM	200
1	✓	HTML	638	335	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:45 AM	200
1	✓	HTML	251	82	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:45 AM	200
1	✓	HTML	453	88	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:45 AM	200
1	✓	HTML	215	4	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:44 AM	200
1	✓	HTML	313	107	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:43 AM	200
1	✓	HTML	722	354	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:43 AM	200
1	✓	HTML	48	8	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:43 AM	200
1	✓	HTML	292	70	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:42 AM	200
1	✓	HTML	168	106	0	0	0	0	0	http://www.foglight.com/.../index.jsp	192.168.1.10	10/07/2014 07:18:42 AM	200

When a hit belongs to a session, the Session Explorer  and Session Detail View  icons appear in the Sessions column. You can view the selected hit within the context of a session and assess the other hits that occurred within the session. For more information about using these views, see [Investigating issues](#).

- 2 Choose an interesting HTML hit to investigate.

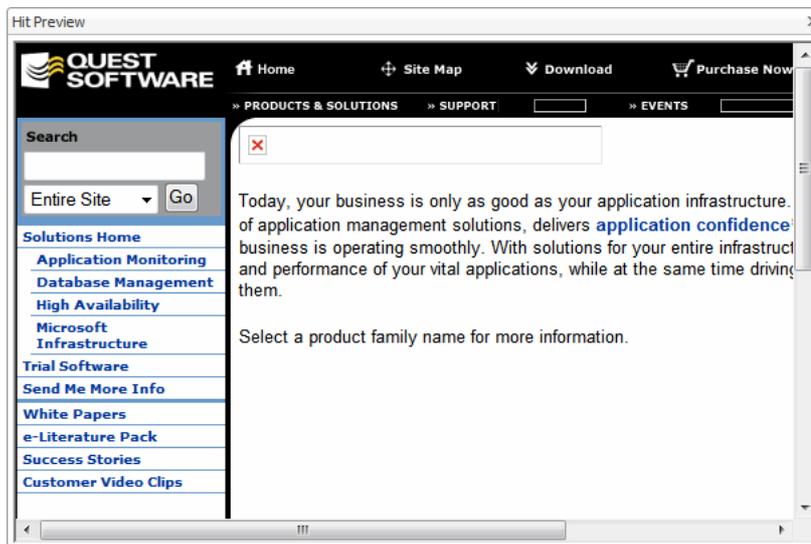
For example, choose a hit that displays one or more of the following characteristics:

- **Status**—look for icons other than the Normal icon. A hit can be set to a non-normal status due to a client or browser error code or when the hit matched some set of conditions defined within a hit analyzer. APM Administrators define and manage hit analyzers.
- **Code**—look for client error codes (400+) or server error codes (500+). Remember though that Web 2.0 applications may not return error codes, because they redirect users to a helpful error page rather than a generic error page. In this case, you need to rely on analyzers catching the errors and setting the hit status to non-normal.
- **End-to-End Time**—very high end-to-end times may indicate a problem with the amount of content on a page or a very slow web server.
- **Back End Time**—very high back end times may indicate a problem with the web server.
- **Exception**—any exceptions should be reported to the application developer.

- 3 To display the contents of the hit, click **Replay**  in the Hits column.

If the hit is an HTML page, you see an approximation of the page as viewed by the user. If you select an image, the Replay window shows the image. If you select a text file such as a CSS file or a JavaScript file, the browser attempts to download the file. In some cases, content may be missing. For more information, see [Understanding what happens when content is unavailable](#).

Figure 26. Hit Preview



- 4 To drill down to the hit details, click **Hit Detail View**  in the Hits column. You can open the view in the current browser window or a new window.

The Hit Detail View opens, displaying details and performance metrics for the hit. As you review the details, you may want to collapse the views you are not interested in. Then you can focus on the details of interest. Click the Client Detail, Metric Updates, and Other Information links to view additional information about the hit.

Figure 27. Hit Details View

Mar 23, 2013 6:17:21 PM UTC

Hit Details View

[Client Details](#) [Metric Updates](#) [Other Information](#)

Content Category	Html	End to End Time	219.201 ms
Hit Status	Ok	Response Total Bytes	28108 bytes
Request Total Bytes	533 bytes	Start Time	03/23/2013 06:01:22 PM
URL Path	/	Stop Time	03/23/2013 06:01:22 PM

Hit Analyzer Matches

Enterprise	✓
Site sections	✓

Request Details

Client IP	192.168.1.100
HTTP Method	GET
Request Content Size	0 bytes
Request Total Bytes	533 bytes
URL	http://www.quest.com/
URL Path	/
URL Scheme and Authority	http://www.quest.com

Request Fields

There Is No Data To Display

Request Headers

Connection	Keep-Alive
Cookie	StandardRequest=State%5F... EMHCFDQVIA14NTMI1N4K1FC1

Response Details

Content Category	Html
Content Type	text/html
HTML Title	Quest Software
HTTP Error	None
HTTP Version	1.0
Response Charset	iso-8859-1
Response Code	200
Response Content Size	27905 bytes
Response Total Bytes	28108 bytes
Server IP	192.168.1.100
Server Port	80
Start Time	03/23/2013 06:01:22 PM
Stop Time	03/23/2013 06:01:22 PM
Virtual Server IP	192.168.1.100
Website	quest.com

Response Headers

Cache-control	private
Connection	Keep-Alive
Content-Length	27905

- 5 If you notice something in the hit details or metrics that looks interesting, you may want to view all the hits by this detail to see if a pattern emerges.

For example, you may suspect that a slow End-to-End Time is typical for the user's region or service provider. To test your hypothesis, you can create a pivot chart for End-to-End Time by Region or ISP. To create a pivot chart, return to the search results. Click **Pivot** . For more information, see [Viewing search results in pivot charts](#).

- 6 To map your results geographically, return to the search results. Click **Map** . For more information, see [Viewing search results in a map](#).

Searching and investigating sessions

You can search for sessions by time range, session identifier, user name, the status of sessions (active or ended), or some combination of these parameters. You can also define match conditions to create very specific searches.

In the Search Sessions dashboard, you can run a simple search or an expert search to find sessions. You can also rerun the last search, save a search, load and run a saved search, or clear search results.

For more information, see the following topics:

- [Defining simple searches for sessions](#)
- [Defining expert searches for sessions](#)
- [Understanding search sessions results](#)
- [Investigating issues reported during real user sessions](#)
- [Viewing search results in a map](#)

- Viewing search results in pivot charts
- Replaying sessions, hits, and sequences
- Repeating the last search
- Saving searches
- Running saved searches
- Clearing search results

Defining simple searches for sessions

A simple search enables you to search for sessions using the most frequently-used search criteria. If you want to search for sessions that occurred within a particular time range or hits that match some set of conditions, you need to define an expert search instead.

To define and run a simple session search:

- 1 In the navigation panel, under Dashboards, click **APM > Search > Sessions**.
- 2 Click **Simple Search**.
- 3 Specify the search criteria.

Table 13. Simple session search criteria

Find sessions that...	In the first list, select the start condition for the search. In the second list, select the time range for the search. If no other options are set, the search returns all sessions occurring within the specified time range. TIP: An APM Administrator can increase or decrease the maximum time range displayed in the time range list through the Configure Advanced Options > Settings dashboard. See the <i>Search Time Range Limit</i> option under the Archiver Query Settings.
are currently	Optional—specify whether you want active or ended sessions. Select this check box and select the state from the list.
Session ID	Optional—search for a session by session identifier. Specify the session identifier you that you want to match.
Username	Optional—search for a real user by user name. Specify the user name (case-insensitive) that you want to match.
Session Hit Count Matching Hit Analyzer	Optional—search for hits that triggered the specified hit analyzer during the session.

Figure 28. Simple Search (sessions) dialog box

4 Click Search.

The Search Sessions table contains the results of the search.

Defining expert searches for sessions

You can run a search using the same options as a simple search. You can also define a time range or some set of conditions, such as session with a specified duration.

NOTE: The Archiver stores session duration in milliseconds, but the UI displays it in seconds. Therefore, if you search sessions based on duration, you may see results that appear to fall outside the search criteria. For example, defining a match condition with “Session Duration > 10” may return search results that appear to match “Session Duration >= 10”. In this case, a session that appears to be equal to 10 seconds actually has a duration greater than 10 seconds, such as 10.4322 seconds, but the UI does not display the decimal places.

To define and run an expert session search:

- 1 In the navigation panel, under Dashboards, click **APM > Search > Session**.
- 2 Click **Expert Search**.

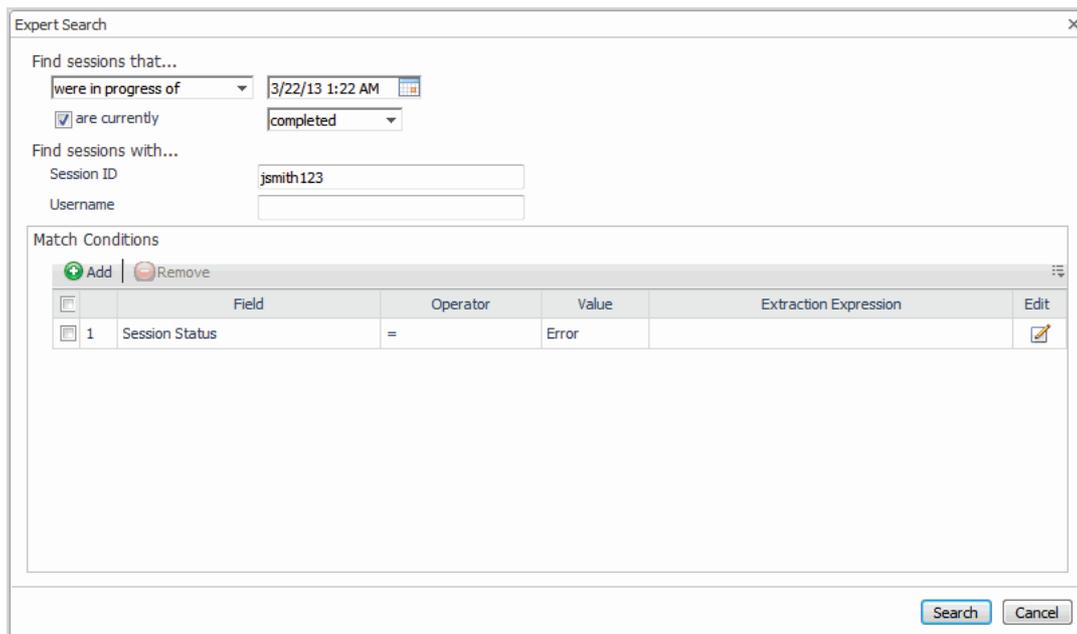
If you defined a simple search before switching to an expert search, the Expert Search dialog box displays the same values for the options you selected in the Simple Search dialog box.

- 3 Specify the search criteria.

Table 14. Expert session search criteria

	In the first list, select the start condition for the search. In the second list, select the time range for the search. If no other options are set, the search returns all sessions occurring within the specified time range.
Find sessions that...	TIP: An APM Administrator can increase or decrease the maximum time range displayed in the time range list through the Configure Advanced Options > Settings dashboard. See the <i>Search Time Range Limit</i> option under the Archiver Query Settings.
are currently	Optional—specify whether you want active or completed sessions. Select this check box and select the state from the list.
Session ID	Optional—search for a session by session identifier. Specify the session identifier you that you want to match.
Username	Optional—search for a real user by user name. Specify the user name (case-insensitive) that you want to match.
Match Conditions	Optional—specify one or more conditions to match. Click Add . You can define a condition based on any detail or metric listed in the Source list. For help creating match conditions, see Defining match conditions for expert searches .

Figure 29. Expert Search (sessions) dialog box



The dialog box is titled "Expert Search" and contains the following sections:

- Find sessions that...**: A dropdown menu set to "were in progress of" and a date/time field set to "3/22/13 1:22 AM".
- are currently**: A checked checkbox and a dropdown menu set to "completed".
- Find sessions with...**: Two text input fields for "Session ID" (containing "jsmith123") and "Username".
- Match Conditions**: A table with columns for Field, Operator, Value, Extraction Expression, and Edit. It contains one condition: "Session Status" = "Error".
- Buttons**: "Search" and "Cancel" buttons at the bottom right.

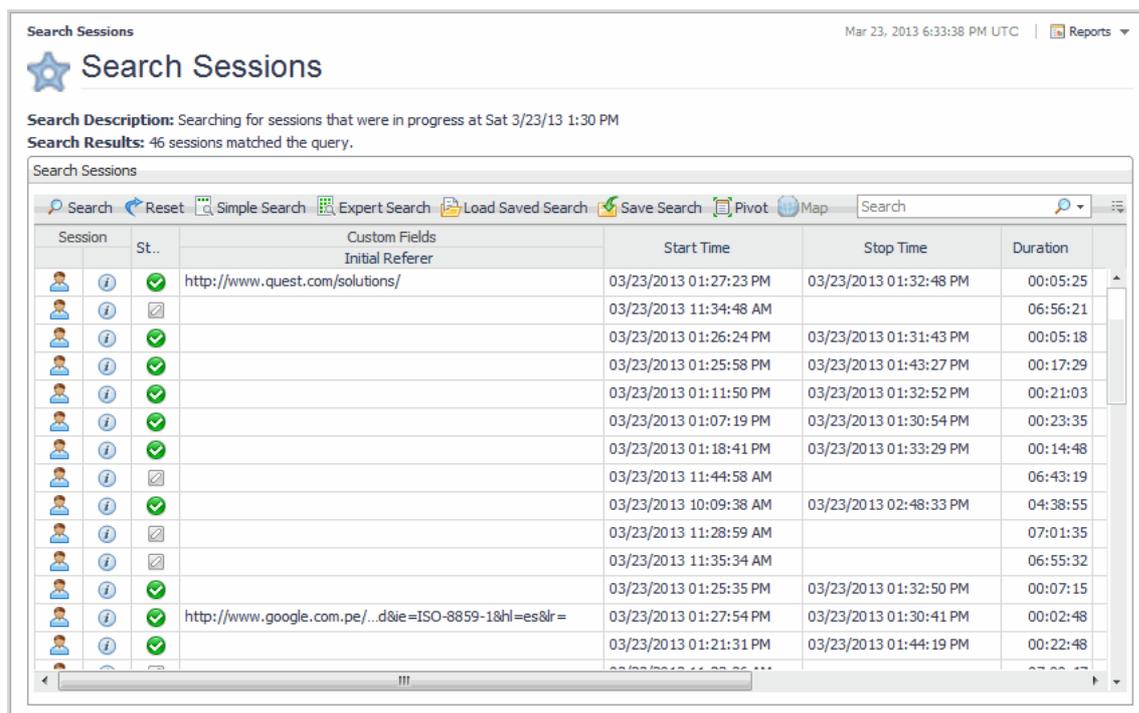
- 4 Click Search.
The Search Sessions table contains the results of the search.
- 5 **Next Steps:** See [Investigating issues](#).

Understanding search sessions results

When the search ends, the results are displayed in the Search Sessions table. The search parameters appear above the table. If no sessions matched the search parameters, the table is empty.

- TIP:** By default, a session search returns a maximum of 200 sessions. An APM Administrator can change this limit using the *Session Search Result Limit* setting in the Configure Advanced Options > Settings dashboard.

Figure 30. Search Sessions dashboard



The Search Sessions table may contain some or all of the following columns. To hide/show columns, click the Customizer  icon (beside the Search field) and select the columns to show.

Table 15. Search Sessions table

Column	Description
Session	The Session Explorer  and Session Detail View  icons appear in this column. You can drill down to session details by clicking these icons.
Status	Indicates the session status using the standard severity icons: <ul style="list-style-type: none">  Normal  Warning  Critical  Fatal  Not available (session is still in progress)
Custom Fields - Initial Referer	Displays the page the user visited just before starting the session (if any).
Start Time	Corresponds to the time the first hit in the session was initiated.
Stop Time	Corresponds to the end time of the last hit in the session.
Duration	Displays the length of the session since the <i>Start Time</i> .
User Name	If username rules are defined, displays the user name associated with the session. For more information, see “Associating user names with user sessions” in the <i>Foglight APM Administration and Configuration Guide</i> .
# Hits	Displays the number of hits contained within the session at the time of the search.
# Pages	Displays the number of pages contained within the session at the time of the search.
# Sequences	Displays the number of sequences contained within the session at the time of the search.

Table 15. Search Sessions table

Column	Description
# Warnings	Displays the number of hits with a warning status contained within the session at the time of the search.
Error Columns	Displays the number of hits with the specified error contained within the session at the time of the search. Show columns for Custom Errors, Reset Errors, HTTP Errors, Client Errors, Server Errors, or Timeout Errors.

Investigating issues reported during real user sessions

When a helpdesk receives reports from real users (internal staff or external users) regarding unexpected errors or slow page performance, technical support staff can use Foglight APM search features to find the problem user sessions. By reviewing what your users experienced, you can form an understanding of what may be causing the problem. You can then escalate the issue to the appropriate person (developer or administrator) for resolution.

For more information, see the following topics:

- [Finding the user session](#)
- [Investigating issues](#)

Finding the user session

You can identify the real user's session using one or more of the following pieces of information as search criteria.

- **Time period**—find out the time period during which the session was active, or find out when the user started or ended their session.
- **Session identifier**—if a user's browser captures the session identifier, instruct the user how to retrieve that identifier.
- **User name**—for applications that require a login, request the user's user name.
- **Client IP address**—for an internal application, request the user's client IP address.
- **Subnet**—for an intranet application, find out the subnet used by the application.
- **City**—if no other identifying details are known, you may need to search sessions by the user's city.
- **Page visited before starting session**—this information can be useful for picking the correct session out of a list of session search results. You can look at the Initial Referer column to find the page the user visited before beginning the session.

The following workflow assumes that you have the session identifier or user name. If you do not, you need to define an expert search and create match conditions using one or more of the other details as your search criteria. For instructions, see [Defining expert searches for sessions](#).

To find the user session:

- 1 Gather information about the user's session.
- 2 Log into Foglight.
- 3 In the navigation panel, under Dashboards, click **APM > Search > Sessions**.
- 4 Click **Simple Search**.
 - a Specify the time period during which the user experienced issues. From the first list, select the state of the session (started, in progress, or ended) during the time period. From the second list, select the time period.

TIP: If no other options are set, the search returns all sessions of the selected state that occurred within the specified time period.

- b Optional—specify whether the session is currently active or complete.
- c Specify either the session identifier or the user name, whichever you have.
- d Click **Search**.

The Search Sessions results table displays the search results.

- 5 If you have only one match, you can begin investigating the session now. Otherwise, you need to pick out the user's session from the results list. If you know the session start time, end time, or the page that the user was looking at before beginning the session, you should be able to select the correct session by looking to those columns in the Search Sessions results table.

Investigating issues

You use the Session Explorer to investigate issues. The Session Explorer contains:

- Complete hit details for the entire HTTP request and response for any hit in the session
- A visual presentation of each page as originally served by the web server
- A visual presentation of each page with user input (forms/links)
- The original HTML source for each page generated by the web server
- Any errors (HTML or other source) detected by analyzers
- Session and sequence durations, hit counts, and other aggregate details

NOTE: This workflow starts from the Search Session results table. However, the process is similar when you drill down from a Real User tile in the Transaction dashboard or when you run a search for hits or sequences.

This workflow presents one way to investigate issues. Your investigation should be guided by the type of problem you are investigating. For example, you may want to skip the session replay and go straight to the hit inspector.

To investigate an issue:

- 1 In the row containing the issue you want to investigate, click **Session Explorer** .

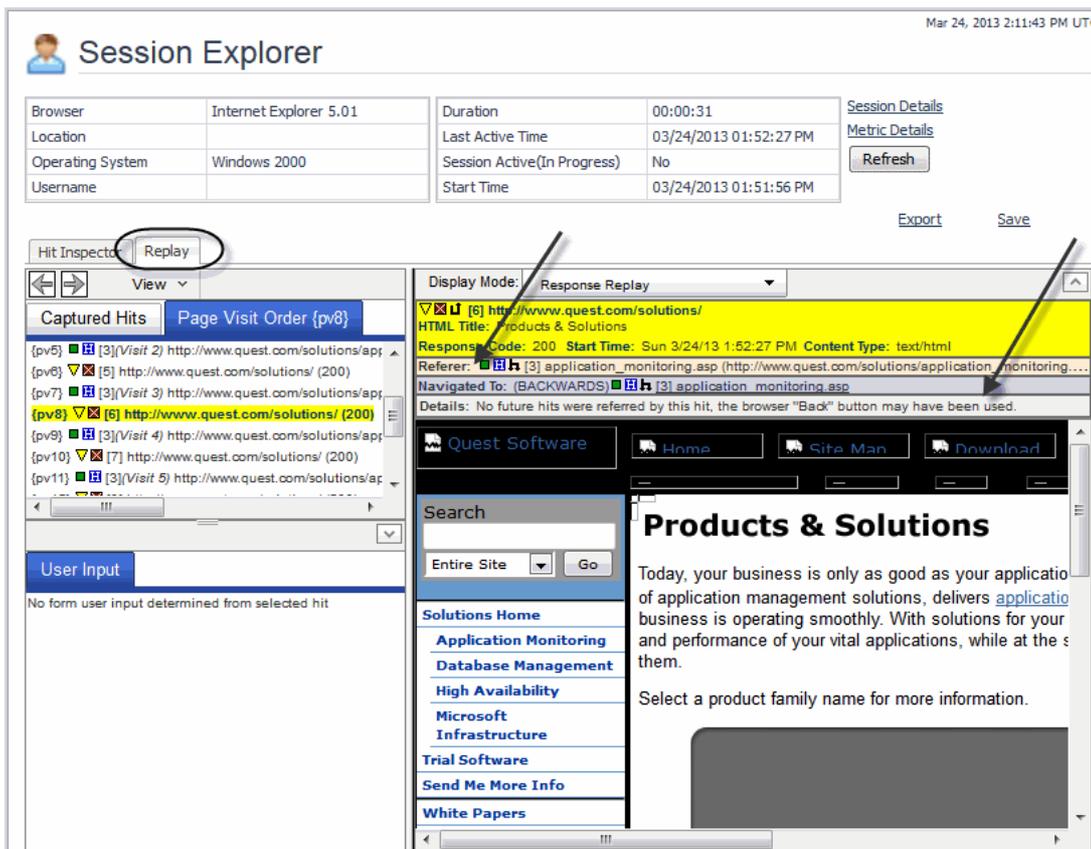
The Session Explorer opens. When opened from the Search Hits results table, the hit displayed is the selected hit. When opened from the Search Sequences or Search Sessions results table, the hit details represent the first hit in the selected sequence or session.

- 2 If not already selected, click the **Replay** tab.

The content associated with the selected hit is displayed. Look for navigation clues in the Referrer/Navigated To sections above the page content. The Details sections may provide additional information. You can switch between Captured Hits (to see all hits) and Page Visit Order (HTML pages). Select different hits in the user's path to view the content they saw.

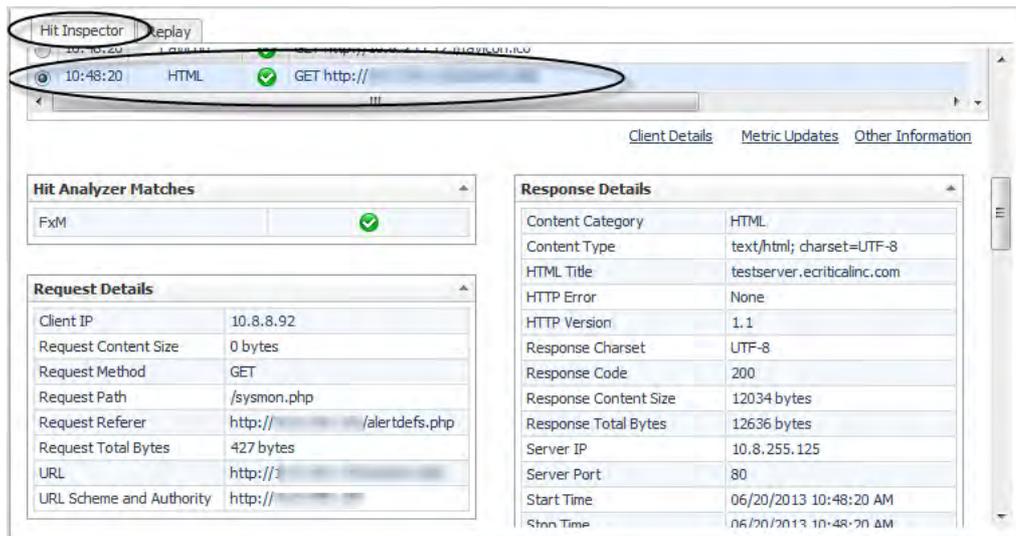
IMPORTANT: Some content may not be shown in the response replay. For more information on missing content and using the features in the Replay tab, see [Replaying sessions, hits, and sequences](#).

Figure 31. Session Explorer dashboard



- 3 To investigate a page further, click the Hit Inspector tab.
- 4 In the list of hits in the session table, look for hits that exhibit symptoms of the problem, such as a hit that displays one or more of the following characteristics:
 - **Status**—look for icons other than the Normal icon. A hit can be set to a non-normal status due to a client or browser error code or when the hit matched some set of conditions defined within a hit analyzer. APM Administrators define and manage hit analyzers.
 - **Code**—look for client error codes (400+) or server error codes (500+). Remember though that Web 2.0 applications may not return error codes, because they redirect users to a helpful error page rather than a generic error page. In this case, you need to rely on analyzers catching the errors and setting the hit status to non-normal.
 - **End-to-End Time**—very high end-to-end times may indicate a problem with the amount of content on a page or a very slow web server.
 - **Back End Time**—very high back end times may indicate a problem with the web server.
 - **Exception**—any exceptions should be reported to the application developer.
- 5 After you identify the hits that contribute to the problem, select each hit in turn and scan the hit details to look for clues about what might be causing the performance issues. Additional details and metrics are available by clicking Metric Updates, Client Details, or Other Information.

Figure 32. Session Explorer Hit Inspector



For example, if the hit status is non-normal but the error code is 200, you can review the hit's details to find out which hit analyzers were triggered. You can pass this information on to an APM Administrator for further investigation and resolution. If the back end time is high, you may want to check the health of the web sites and endpoints in your monitored environment, especially if you are having many users reporting similar issues.

- 6 If you suspect that poor performance is localized to a city, region, or country, you can create a map using the search results. In the search results, click **Map** . For more information, see [Viewing search results in a map](#).
- 7 If many real users are reporting the same issue, it may be helpful to create a pivot chart that aggregates data for all users. Return to the search results. Click **Pivot** . For more information, see [Viewing search results in pivot charts](#).

Searching and investigating sequences

If your APM Administrator configured sequence analyzers, you can search for sequences created by a selected analyzer. You can also specify a time range, sequence state (active or completed), session identifier, sequence status (OK, warning, error), or some combination of these search parameters. You can define match conditions to create very specific searches.

- NOTE:** If you want a high-level, graphical view of aggregated sequence data, start from the Sequence Explorer dashboard. From there, you can navigate to the Search Sequences dashboard described in this section. For more information, see [Assessing real user experiences during key sequences](#).

In the Search Sequences dashboard, you can run a simple search or an expert search to find sequences. You can also rerun the last search, save a search, load and run a saved search, or clear search results.

For more information, see the following topics:

- [Defining simple searches for sequences](#)
- [Defining expert searches for sequences](#)
- [Understanding search sequences results](#)
- [Investigating sequence results](#)
- [Replaying sessions, hits, and sequences](#)
- [Viewing search results in pivot charts](#)

- Repeating the last search
- Saving searches
- Running saved searches
- Clearing search results

Defining simple searches for sequences

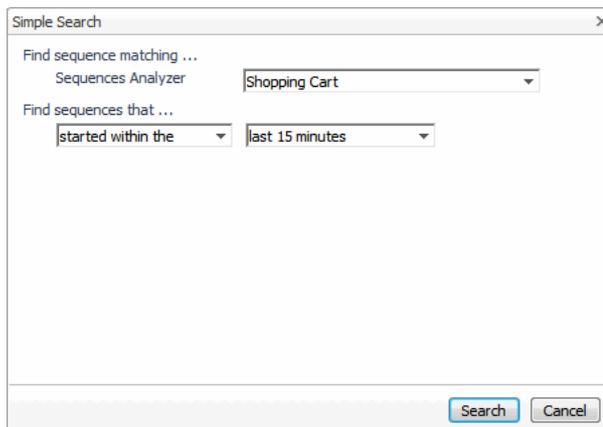
A simple search returns sequences that were active at the time period you specify. If you are not the designer of the sequence analyzers, you should find out the names of the sequence analyzers that track the sequences you are interested in. APM Administrators define sequence analyzers.

To define and run an simple sequence search:

- 1 In the navigation panel, under Dashboards, click **APM > Search > Sequences**.
- 2 Click **Simple Search**.
- 3 Select a sequence analyzer that captures the sequences you want to find.
The options for the sequence analyzer appear.
- 4 Under **Find sequences that**, select the time criteria for the sequences.

TIP: An APM Administrator can increase or decrease the maximum time range displayed in the time range list through the **Configure Advanced Options > Settings** dashboard. See the *Search Time Range Limit* option under the Archiver Query Settings.

Figure 33. Simple Search (sequences) dialog box



- 5 Click **Search**.

The Search Sequences table contains all sequences occurring within the specified time range.

Defining expert searches for sequences

You can run an expert search using the same options as a simple search. You can also specify whether the sequence was active or completed. You can further refine the search by specifying a particular user session, sequence status, or match conditions.

If you are not the designer of the sequence analyzers, you should find out the names of the sequence analyzers that track the sequences you are interested in. APM Administrators define sequence analyzers.

To define and run an expert sequence search:

- 1 In the navigation panel, under Dashboards, click **APM > Search > Sequences**.
- 2 Click **Expert Search**.

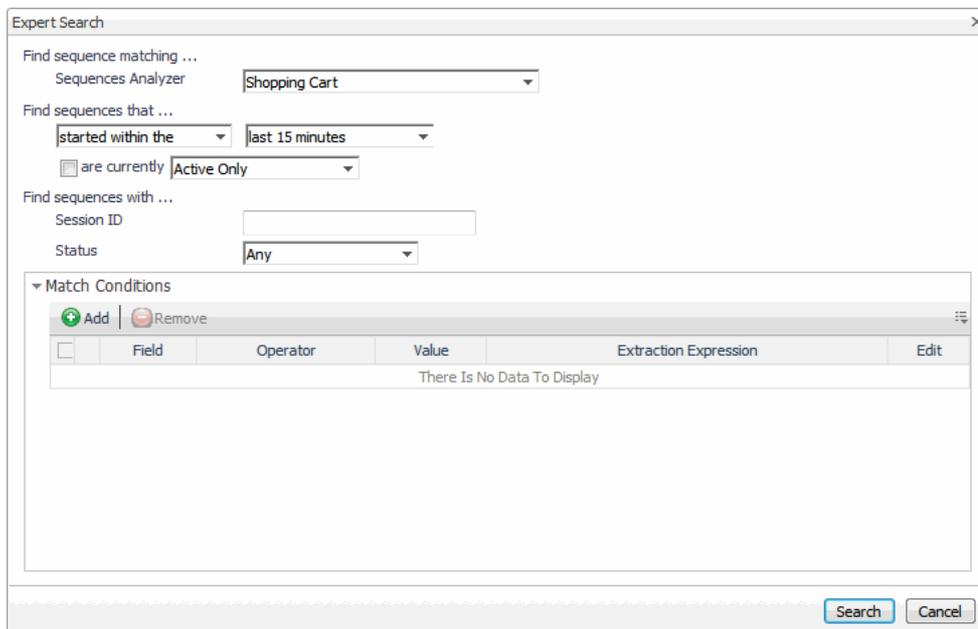
If you defined a simple search before switching to an expert search, the Expert Search dialog box displays the same sequence analyzer and the same time criteria you selected in the Simple Search dialog box. Advanced options are also displayed.

- 3 Select a sequence analyzer, and then specify the search criteria.

Table 16. Expert sequence search criteria

Sequence Analyzer	Specify the name of the sequence analyzer that captures the sequences you want to find.
Find sequences that...	In the first list, select the start condition for the search. In the second list, select the time range for the search. The search returns all sequences occurring within the specified time range. TIP: An APM Administrator can increase or decrease the maximum time range displayed in the time range list through the <i>Configure Advanced Options > Settings</i> dashboard. See the <i>Search Time Range Limit</i> option under the <i>Archiver Query Settings</i> .
are currently	Optional—specify whether you want active or completed sequences. Select this check box and select the state from the list.
Session ID	Optional—search for sequences by session identifier. Specify the session identifier you that you want to match.
Status	Optional—search for sequences by status (OK, Warning, Error). Select the status from the list.
Match Conditions	Optional—specify one or more conditions to match. Click Add . You can define a condition based on any detail or metric listed in the Source list. For help creating match conditions, see Defining match conditions for expert searches .

Figure 34. Expert Search (sequence) dialog box



- 4 Click **Search**.

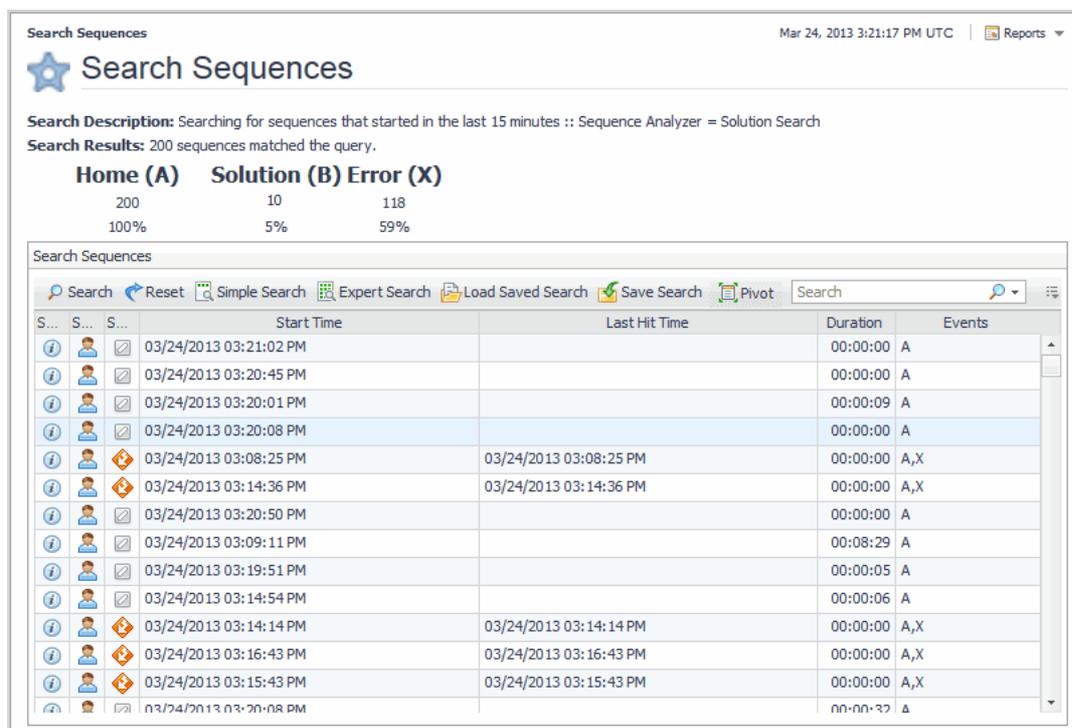
The Search Sequences table contains the results of the search.

Understanding search sequences results

When the search ends, the results are displayed in the Search Sequences table. The search parameters appear above the table. If no sequences matched the search parameters, the table is empty. Events are summarized by name and include the number of users who reached each step.

- TIP:** By default, a sequence search returns a maximum of 200 sequences. An APM Administrator can change this limit using the Sequence Search Result Limit setting in the Configure Advanced Options > Settings dashboard.

Figure 35. Search Sequences dashboard



The Search Sequences table may contain some or all of the following columns. To hide/show columns, click the Customizer icon (beside the Search field) and select the columns to show.

Table 17. Search Sequences table

Column	Description
Session	When a sequence belongs to a session, the Session Explorer and Session Detail View icons appear in this column. You can view session details by clicking these icons.
Status	Indicates the sequence status using the standard severity icons: <ul style="list-style-type: none"> Normal Warning Critical Fatal Not available (sequence is still in progress)

Table 17. Search Sequences table

Column	Description
Custom Fields	Displays the custom fields updated by analyzers that matched a sequence. NOTE: For a custom field to appear in search results, the custom field's Storage option must be set to <i>Show in search results</i> or <i>First column in search results</i> . See "Defining custom fields" in the online help.
Start Time	Corresponds to the time the first hit in the sequence was initiated.
Stop Time	Corresponds to the end time of the last hit in the sequence.
Duration	Displays the length of the sequence since the <i>Start Time</i> .
Events	Events that occurred within a sequence.

Investigating sequence results

This workflow walks through how to use the data in the Search Sequences table. You may want to save your searches so that you can quickly rerun them to monitor performance on an ongoing basis.

To investigate sequences from search results:

- 1 From the Search Sequences dashboard, run a search.
 - [Running saved searches](#)
 - [Repeating the last search](#)
 - [Defining simple searches for sequences](#)
 - [Defining expert searches for sequences](#)

When a search matches sequences in the database, the results table displays the sequences.

- 2 To identify sequences that may warrant further investigation, review the following columns.
 - **Status**—look for icons other than the Normal icon. A sequence event can be used to set the status of a sequence. APM Administrators define and manage sequence analyzers.
 - **Events**—look for patterns across all sequences. Did many users abandon the critical path at the same event? Why might that be?
 - **Duration**—click this column heading to sort the sequences from longest to shortest. You may want to investigate why some sequences were extra long (was it due to slow response times?) or very short (did the user abandon the critical path or was the sequence terminated by an error?).
 - **Custom Fields**—custom fields can help you understand the placement of a sequence within the user's entire session. The Initial Referer tells you which page the user visited before starting the critical path.
- 3 Select a sequence to investigate and click its **Session Explorer**  icon.
The Session Explorer opens.
- 4 You can explore the sequence in the same way you explore a session. See [Investigating issues reported during real user sessions](#).
- 5 If you suspect that poor performance is localized to a city, region, or country, you can create a map using the search results. In the search results, click **Map** . For more information, see [Viewing search results in a map](#).
- 6 If many sequences reflect the same issue, it may be helpful to create a pivot chart that aggregates data for all users. Return to the search results. Click **Pivot** . For more information, see [Viewing search results in pivot charts](#).

Managing searches

In all the Search dashboards, you can save and rerun searches. You can also clear search results from the table.

For more information, see the following topics:

- [Repeating the last search](#)
- [Saving searches](#)
- [Running saved searches](#)
- [Clearing search results](#)
- [Defining match conditions for expert searches](#)

Repeating the last search

To repeat the last search performed in a Search dashboard, click **Search**. The search parameters appear at the top of the dashboard beside Search Description, and the number of matches appears beside Search Results. The matches (if any) are listed in the table.

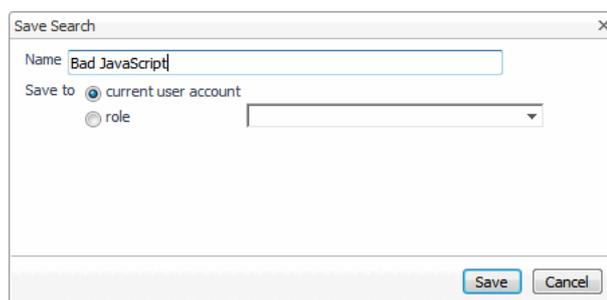
Saving searches

For the searches that you perform frequently, consider saving them. You can shared saved searches among people with the same user role. For example, an APM Administrator can create searches useful to APM Operators and share them by selecting that user role.

To save a search:

- 1 Define and run a search.
- 2 Click **Save Search**.
The Save Search dialog box opens.
- 3 Specify a name for the search.
- 4 Choose whether you want the search available only to you (current user account) or available to everyone with a specific user role. In the latter case, select the user role from the list.

Figure 36. Save Search dialog box



- 5 Click **Save**.
The dialog box closes. On the Search Hits dashboard, the parameters for the loaded search appear beside Search Description. The search results are not updated yet.
- 6 To run the loaded search, click **Search**.
The search results display matches (if any).

Running saved searches

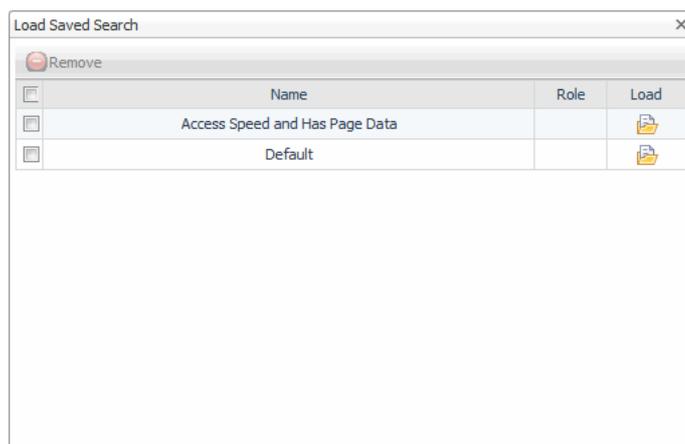
Saved searches can help ensure that you run consistent searches. For example, you may run a search, find data issues, make a configuration change, and then want to rerun the same search. If you save the initial search, you can be sure that the second set of results reflect just the configuration change, not any inadvertent changes in the search parameters.

To run a saved search:

- 1 Click **Load Saved Search**.

The Load Saved Search dialog box opens.

Figure 37. Load Saved Search dialog box



- 2 In the row containing the search you want to run, click **Load**

The dialog box closes. On the Search Hits dashboard, the parameters for the loaded search appear beside Search Description. The search results are not updated yet.

- 3 To run the loaded search, click **Search**.

The search results display matches (if any).

Clearing search results

To clear the search results in a Search dashboard, click **Reset**. This action also resets the Search button to the default search parameters.

Defining match conditions for expert searches

You can create searches that return very specific results by defining match conditions. Match conditions enable you to search on almost any detail or performance metric.

When creating an expert search with multiple conditions, logical operators are applied depending on the specified conditions.

- When conditions match *different* details, a logical AND operator joins the conditions. For example, if you define a hit search using the conditions *City = Madison, WI (US)* and *Browser Category = Internet Explorer*, data must match both the specified city and browser to be returned by the search.
- When conditions match the *same* detail, an OR operator joins the conditions. For example, if you define a hit search using the conditions *City = Madison, WI (US)* and *City = Boulder, CO (US)*, only one of the conditions have to match. The search returns capture data originating from either one of the cities.

In a complex search where *City = Madison, WI (US)*, *City = Boulder, CO (US)*, and *Browser Category = Internet Explorer*, the search logic looks like this:

```
("City = Madison, WI (US) OR Boulder, CO (US)") AND ("BrowserCategory = Internet Explorer")
```

To add or edit a match condition for expert searches:

- 1 In the Match Conditions area of the Expert Search dialog box, do one of the following:
 - To add a new condition, click **Add**.
 - To edit a condition, click its **Edit**  icon.
- 2 Specify the search criteria.

Table 18. Match condition search criteria

Source	Select the type of web traffic matched by the condition. For example, End to End Time, Request Field, Browser, and so on. NOTE: The other fields change depending on the selected Source.
Source Detail	If available, select some detail to further refine the Source selection. For example, instead of matching all Request Fields, you can specify only <code>Order.BillShip</code> .
Operator	Select an operator that performs the type of match you want to make. Only the operators that make sense for a selected Source type are available.
Value	Specify a numeric or text value (as appropriate). For example, you can specify that a match occurs when Client Time (ms) is greater than 600. Or, for Country, you can select a text string from a list, such as "Canada (CA)".

- 3 Click **Save**.

Replaying sessions, hits, and sequences

Often it is easier to understand real user data when you can see the page your user viewed. Foglight enables you to replay interesting hits, alone or in the context of a sequence or session. The Replay browser lives in the Session Explorer. From the Replay browser, you can navigate among the hits in a session, see the pages and hit content viewed by your user, save sessions for review later, and export sessions to share with colleagues.

 **NOTE:** To understand how the Replay browser supports investigating issues, see [Investigating issues](#).

For more information, see the following topics:

- [Introducing the Replay browser](#)
- [Changing how content is displayed](#)
- [Customizing the Selection pane](#)
- [Understanding what happens when content is unavailable](#)
- [Using the Hit Inspector](#)
- [Managing saved sessions](#)

Introducing the Replay browser

You can open the Session Explorer from any search result that displays the Session Explorer  icon.

To open the Replay browser:

- 1 In the search results, click the **Session Explorer**  icon, and select whether to open the Session Explorer in the current browser window or a new window.

The Session Explorer opens. The active tab is the tab displayed the last time you opened the Session Explorer.

- 2 If not already selected, click the **Replay** tab.

The Replay browser displays the selected hit. The following image and table identify the elements in the Replay browser.

Figure 38. Replay browser

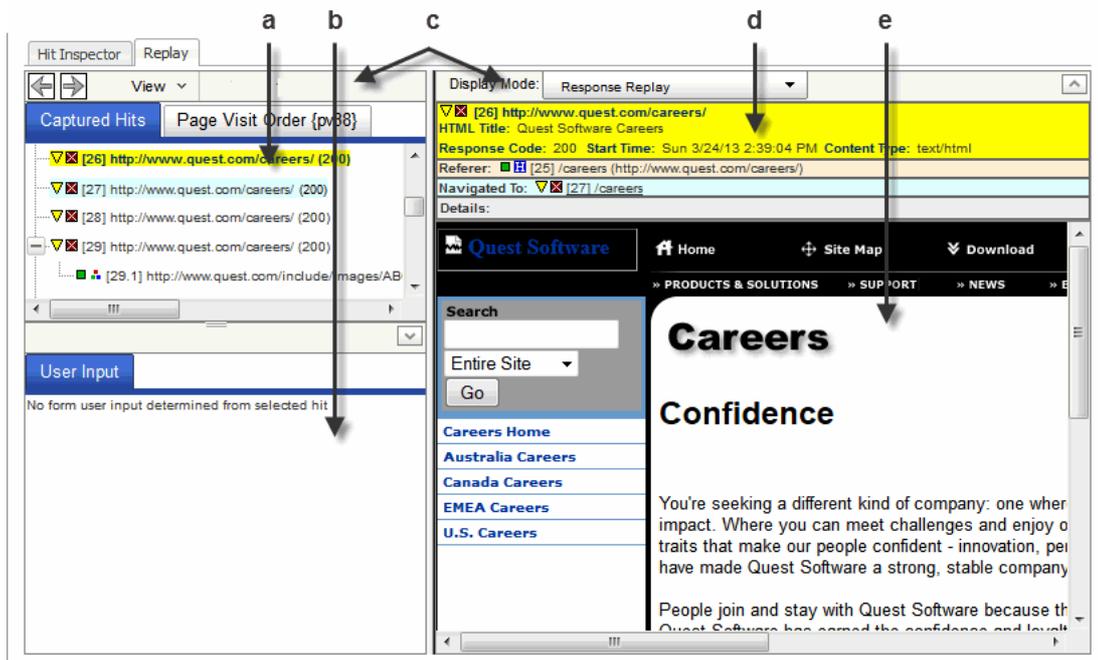


Table 19. Replay browser elements

Element	Description
a Selection pane	Displays either a list of hits or a list of pages. Select a hit or page to view it in the Replay pane.
b User Input pane	Displays the input values entered by the user in form fields, or the buttons or links clicked.
c Replay menu	Navigate between pages, control what is displayed in the Replay browser, or export sessions from here to replay later.
d Details pane	Displays details about the hit or page.
e Content pane	Displays the content for the selected hit or page.

- 3 To work with hits, in the Selection pane, select the Captured Hits tab.

By default, the list includes HTML hits as well as hits for other resources, such as images, text, and JavaScript.

- 4 Click a hit to view its details and content.

The hit's details appear in the Details pane, and the hit's content appears in the Content pane.

- 5 To work with pages, in the Selection pane, select the Page Visit Order tab.

The pages are listed in the order in which the real user viewed them. For replay purposes, a page is defined as having both page data and HTML.

NOTE: Pages without HTML do not qualify for page replay. For example, applications such as Siebel, PeopleSoft, and SharePoint®, may contain pages without HTML. In addition, pages identified by user-defined URL classifiers may not qualify. In this case, use the Captured Hits tab instead.

- 6 Click a page to view its details and content.

- 7 To page through the user's session, select each page in turn or use the navigation arrows on the Replay menu.

- 8 If the session you are viewing is still in progress, periodically click **Refresh** to update the data in the Session Explorer.
- 9 **Optional**—customize the Replay browser.
 - **Content pane:** [Changing how content is displayed](#)
 - **Selection pane:** [Customizing the Selection pane](#)

Changing how content is displayed

You can change what you see in the Content pane by selecting a different Display Mode. The following table describes the kinds of views available.

Table 20. Replay browser display modes

Display Mode Option	Setting the Option
Response Replay	Select to view an approximation of the content as the real user originally viewed it. For more information, see Understanding what happens when content is unavailable .
Response Replay (Show Submitted Input)	Select to view an approximation of the content as the real user originally viewed it, <i>plus</i> the final values for all form fields and any links or buttons that were clicked. For more information, see Understanding what happens when content is unavailable . NOTE: Excludes forms or links manipulated by JavaScript on the client browser, including actions that are purely client-side.
Response Source	For HTML hits, select this display mode to see the source code that was captured. This mode is useful for debugging dynamic web applications. If a selected hit is not an HTML page, displays the same view as <i>Response Replay</i> mode.
Hit Details	Select to view the network and HTTP details about a selected hit, including response time, hit analysis, request and response fields, and headers, cookies, and Archiver details.
Request Content Body	For hits that use POST as the HTTP request method, select this display mode to view the HTTP request message body as text. Useful for viewing data POST-ed from the browser, including special request content-types (for example, XML and JSON formats).
Instrumentation	Select to view raw instrumentation data. Requires that an APM Administrator included a call to the Foglight instrumentation JavaScript library on the monitored web site or application. For more information, see “Capturing traffic outside the network” in the <i>Foglight APM Administration and Configuration Guide</i> .

Customizing the Selection pane

You can customize the Selection pane using the View menu options. The following table summarizes the options.

Table 21. Selection pane options

View Menu Option	Setting the Option
Show Only HTML Hits	Select to show only HTML hits. Deselect (default) to show all hits.
Display Page Titles for HTML Hits	Select to show the HTML page title (when available). Deselect (default) to show the URL path.

Table 21. Selection pane options

View Menu Option	Setting the Option
Display Full URL for Hit Labels	Select (default) to show the full URL path. Deselect to show only the file name.
Expand All	Select to expand all nested elements in a list of hits.
Collapse All	Select to collapse all nested elements in a list of hits.
Expand Errors/Warnings	Select to expand nested elements marked as errors or warnings.
Enable Tooltips	Select to enable tooltips containing hit details for the hits.

Understanding what happens when content is unavailable

Sometimes content is not available in the captured data. For example, content may have been cached in an earlier session and therefore was not returned as a hit in the current session. Depending on how your APM Administrator configured replay settings, missing content may be shown as broken links, replaced with resources of the same name retrieved from the live web server (default), or replaced by static page resources. For more information, see the *When Element Content not Available* setting under “Replay settings” in the *Foglight APM Administration and Configuration Guide* online help.

Using the Hit Inspector

The Hit Inspector shows content similar to the Hit Detail View, but within the context of a session. When you select a hit in the table, hit details and metrics appear below the table. As you review the details, you may want to collapse the views you are not interested in. Then you can focus on the details of interest. Click the Client Detail, Metric Updates, and Other Information links to view additional information about the hit.

To review hit details from the Session Explorer:

- 1 Click the Hit Inspector tab.
- 2 In the first column, select the radio button for the hit you want to investigate.
Hit details appear below the table.

Figure 39. Session Explorer, Hit Inspector tab

The screenshot shows the Session Explorer interface with the Hit Inspector tab selected. The top section displays session metadata in a table:

Browser	Chrome 27.0	Duration	01:11:09	Session Details
Location		Last Active Time		Metric Details
Operating System	Windows 7	Session Active(In Progress)	Yes	Refresh
Username		Start Time	06/20/2013 09:51:01 AM	

Below this is a Hit Inspector timeline showing a hit at 10:48:20 with a status of HTML and a successful GET request. A black oval highlights this hit. To the right of the timeline are buttons for 'Hit Inspector' and 'Replay'. Further right are 'Export' and 'Save' buttons.

The bottom section is divided into two panels:

- Hit Analyzer Matches:** Shows a match for 'Fxm' with a green checkmark.
- Request Details:** A table with the following data:

Client IP	10.8.8.92
Request Content Size	0 bytes
Request Method	GET
Request Path	/sysmon.php
Request Referer	http://[redacted]/alertdefs.php
Request Total Bytes	427 bytes
URL	http://[redacted]
URL Scheme and Authority	http://[redacted]
- Response Details:** A table with the following data:

Content Category	HTML
Content Type	text/html; charset=UTF-8
HTML Title	testserver.ecriticalinc.com
HTTP Error	None
HTTP Version	1.1
Response Charset	UTF-8
Response Code	200
Response Content Size	12034 bytes
Response Total Bytes	12636 bytes
Server IP	10.8.255.125
Server Port	80
Start Time	06/20/2013 10:48:20 AM
Stop Time	06/20/2013 10:48:20 AM

Managing saved sessions

As you investigate sessions in the Session Explorer, you can save interesting sessions to review later. You can also export sessions for archive purposes or to send to Dell Support. To replay an exported session, import it into Foglight. You replay saved and imported sessions in the Session Explorer.

For more information, see the following topics:

- [Saving sessions](#)
- [Exporting sessions](#)
- [Importing sessions](#)
- [Replaying saved sessions](#)

Saving sessions

While looking at a session in the Session Explorer, if you find an issue that needs further investigation, save the session. You may also want to save a session to use as a baseline before performance improvements are made to a web application. When escalating an issue, include the names of relevant saved sessions. The person responsible for resolving issues can review the sessions in Foglight and use the session data to help solve the problem.

Saved sessions are shared among all Foglight users with the role of APM Administrator or APM Operator. When naming sessions, you may want to include your name along with other identifying information for the session.

CAUTION: If you have the role of APM Sensitive Data Viewer, the saved session may contain sensitive data. To avoid saving sensitive data, log in as a user that does not have the APM Sensitive Data Viewer role enabled. Saved sessions containing sensitive data can be viewed only by users with the APM Sensitive Data Viewer role.

To save the current session:

- 1 In the Session Explorer, click **Save**.
- 2 In the Save Session Name field, type a name for the session.
- 3 Click **Save**.
A message box confirms when the save file has been created.
- 4 Click **OK**.

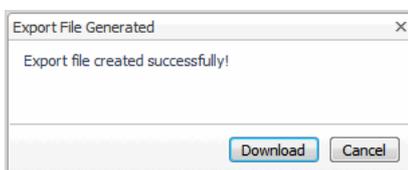
Exporting sessions

Because saved sessions are shared, anyone can delete saved sessions. To back up your saved sessions, or to keep sessions for future reference, export the sessions to a local drive. Exported sessions are also a useful tool for Dell Support to diagnose data issues. Sessions are exported in ZIP format.

CAUTION: If you have the role of APM Sensitive Data Viewer, the exported session may contain sensitive data. To avoid exporting sensitive data, log in as a user that does not have the APM Sensitive Data Viewer role enabled. Imported sessions containing sensitive data can be viewed only by users with the APM Sensitive Data Viewer role.

To export a session:

- 1 In the Session Explorer, click **Export**.
A message box confirms when the export file has been created, and prompts you to download the ZIP file.



- 2 Click **Download** and save the file to your local drive.

Importing sessions

Imported sessions appear in the same list as all saved sessions. When naming imported sessions, you may want to include your name along with other identifying information for the session.

To import a session:

- 1 In the navigation panel, under Dashboards, click **APM > Search > Saved Sessions**.
- 2 Click **Import**.
- 3 Click **Choose file to import**.
- 4 Navigate to and select the session ZIP file, and click **Confirm**.
- 5 In the Session Name field, type a name for the session.
- 6 Click **Import**.

Replaying saved sessions

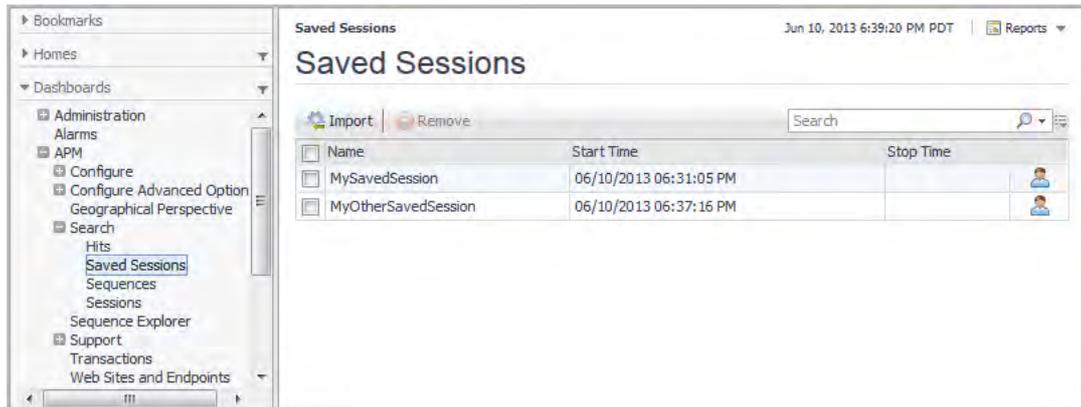
The Saved Sessions dashboard contains all sessions saved or imported by Foglight users with the role of APM Administrator or APM Operator.

To replay a saved session:

- 1 In the navigation panel, under Dashboards, click **APM > Search > Saved Sessions**.

The Saved Sessions dashboard displays a list of saved and imported sessions, including their start times (for all sessions) and stop times (for completed sessions).

Figure 40. Saved Sessions dashboard



- 2 Find the session you want to view and click its **Session Explorer** icon.
The Session Explorer opens and displays the saved session.
- 3 Interact with the session as usual.

Visualizing search results

It can often be helpful to visualize search results as aggregated values in a map or in a pivot chart. For more information, see the following topics:

- [Viewing search results in a map](#)
- [Viewing search results in pivot charts](#)
- [Publishing maps and charts to custom dashboards](#)

Viewing search results in a map

From the Search dashboards, you can gain a geographical perspective on the current search results with maps. Maps can help you visualize an aggregate detail by country, region, or city. For example, a map can help you answer a question such as “Given these search results, which cities had the highest number of errors?” Maps are available for hits and sessions.

TIP: If maps do not display in your browser—for example, if you are using Microsoft® Internet Explorer® version 8 or earlier—try using a different browser. For a list of supported browsers, see the *Foglight System Requirements and Platform Support Guide*.

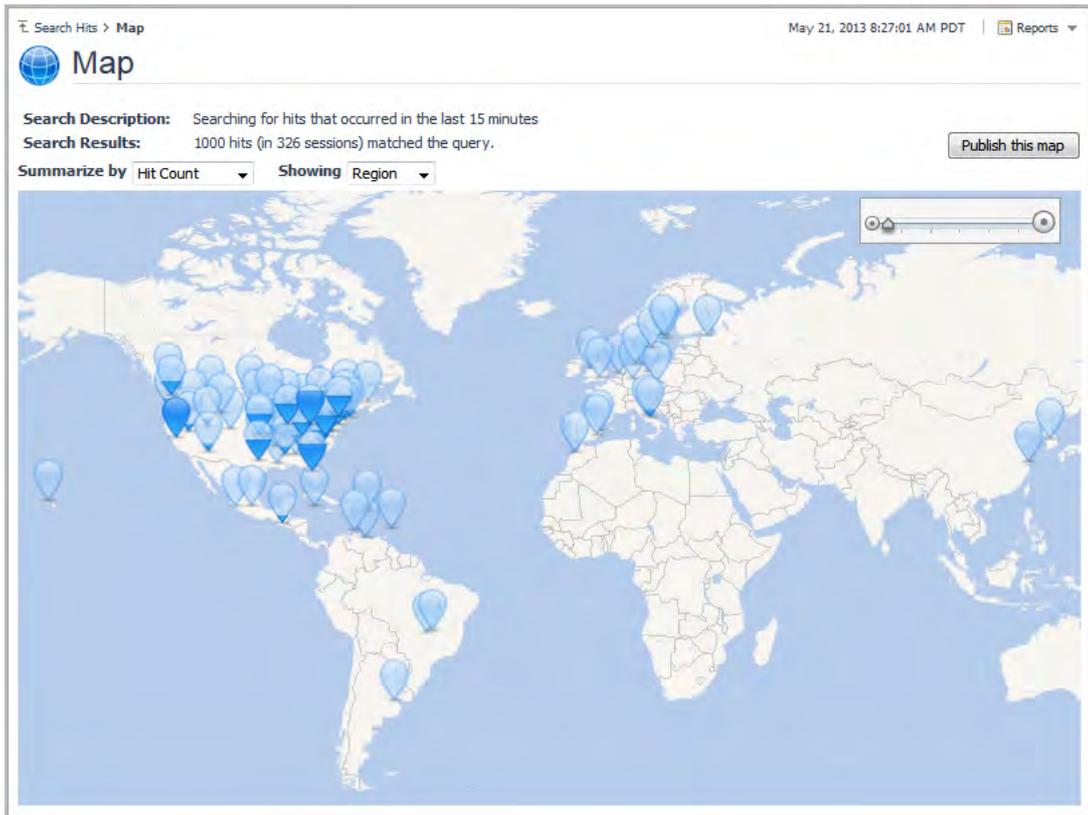
You interact with a search results map in the much the same way as the Geographical Perspective dashboard. For more information, see [Viewing real user activity from a geographical perspective](#).

To view an aggregated metric in a map:

- 1 Define and run a search. For instructions, see [Searching APM data](#).
- 2 From the search results, click **Map** .

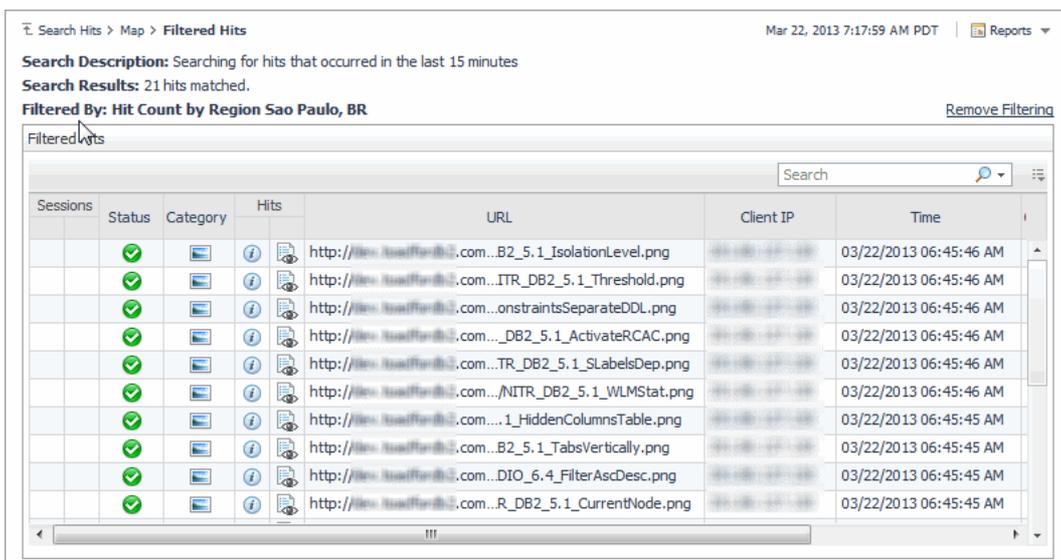
The Map dashboard opens, displaying a map of the world. By default, the aggregated metric is Hit Count and it is shown by Region. The fill-level in the pins shows which regions had comparatively higher and lower hit counts. A pin entirely filled with dark blue represents the region with the highest hit count.

Figure 41. Map dashboard



- 3 You can change the map criteria. Select a new metric from the Summarize By list and/or a new location level from the Showing list.
- 4 To display the search results represented by a pin, click the pin.

Figure 42. Map > Filtered Hits dashboard



- 5 If you want to see all search results in this dashboard, click **Remove Filtering**. You can return to the subset of results by clicking **Restore Filtering**.
- 6 Use the breadcrumb trail to return to the Map dashboard.

- If you want to save a map for use in a custom dashboard, click **Publish**. For more information, see [Publishing maps and charts to custom dashboards](#).

Viewing search results in pivot charts

Pivot charts help you to visualize the composition of an aggregated metric by pivot category, Request Referer, or Response HTML Title. For example, the default pivot charts can help you answer a question such as “Given these search results, which browsers had the highest hit counts?”

IMPORTANT: You do not need to enable pivot categories to generate pivot charts. Pivot charts are generated on-the-fly for the current search results based on captured data stored in the Archiver database. The resulting pivot values are for display purposes only; they are not saved anywhere. In contrast, pivot categories create sets of topology objects to store pivot values in the Foglight database for other purposes, such as higher-level views and reports.

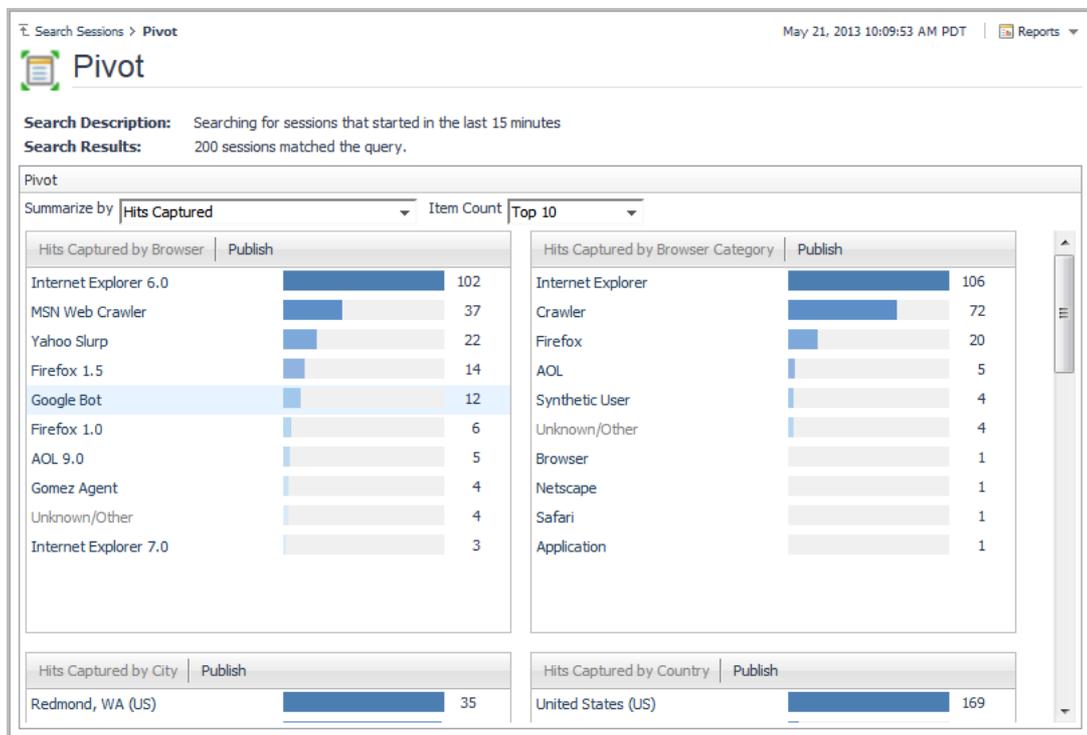
You can quickly view a set of charts showing the aggregated values for the Hit Count metric by various hit, session, or sequence details, depending on the search results. You can update the charts to represent a different aggregated metric. You can also change whether you are seeing the highest value metrics (Top) or lowest value metrics (Bottom), and how many of each you see in the charts. By default, you see the Top 10 values.

To view an aggregated metric in pivot charts:

- Define and run a search. For instructions, see [Searching APM data](#).
- From the search results, click **Pivot**.

The Pivot dashboard opens, with a set of bar charts displayed. The first one shows the Top 10 browsers based on aggregated values for the Hit Count metric.

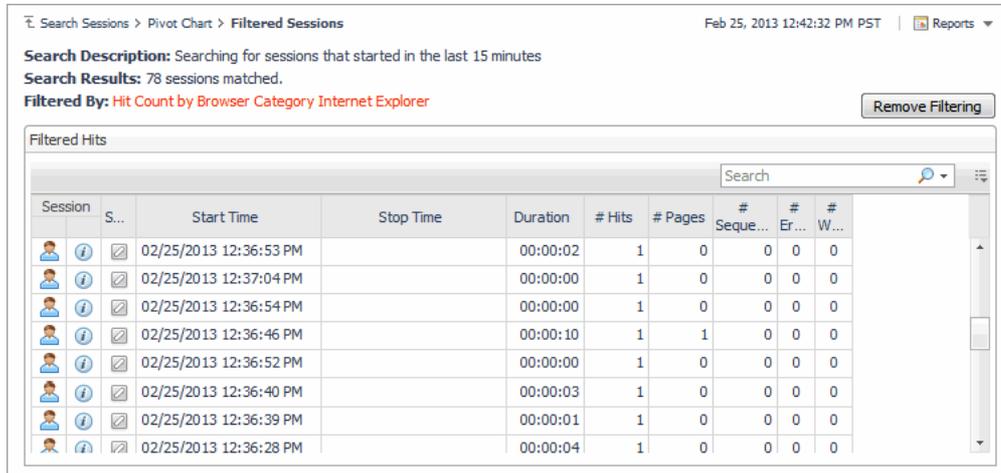
Figure 43. Pivot dashboard



- Scroll down to review the other available charts.

- To change the aggregated metric used to populate the pivot charts, select the new metric from the Summarize By list.
- To show something other than the Top 10 results (default), select a new criteria from the Item Count list.
- To display the search results that are represented by a bar in the chart, click the bar.

Figure 44. Pivot Chart > Filtered Sessions dashboard



- If you want to see all search results in this dashboard, click **Remove Filtering**. You can return to the subset of results by clicking **Restore Filtering**.
- Use the breadcrumb trail to return to the Pivot dashboard.
- If you want to save a chart for use in a custom dashboard, click **Publish**. For more information, see [Publishing maps and charts to custom dashboards](#).

Publishing maps and charts to custom dashboards

You can save a map or pivot chart as a view element, which you can then place on a custom dashboard. For more information on custom dashboards, including how to use them, see “Custom dashboard” in the *Foglight User Help* online help.

For more information, see the following topics:

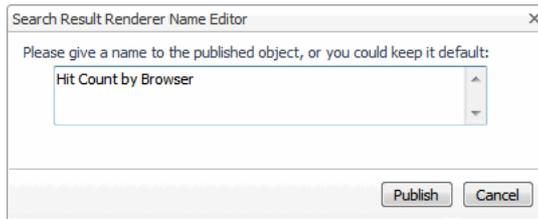
- [Publishing maps and charts](#)
- [Adding maps or charts to a custom dashboard](#)
- [Managing published maps and charts](#)

Publishing maps and charts

To publish a map or chart:

- On the Map or Pivot Chart dashboard, in the area containing the map or chart you want to save as a view element, click **Publish**.
- Keep the default name or specify your own.

Figure 45. Search Result Renderer Name Editor dialog box



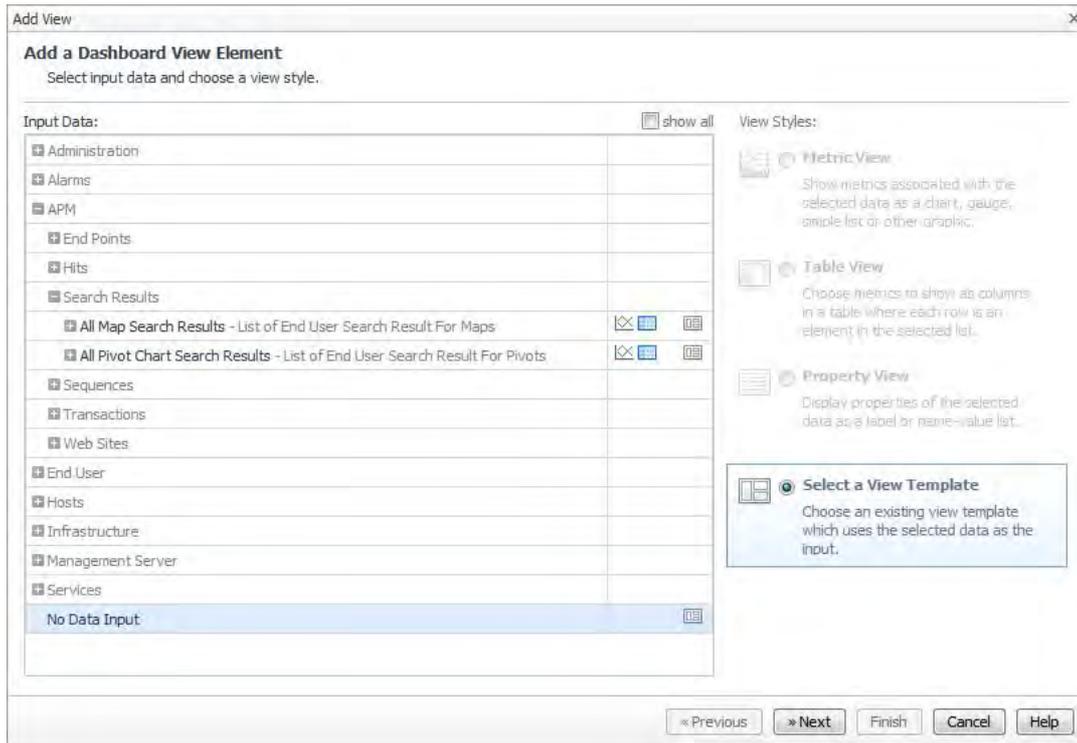
- 3 Click **Publish**.

Adding maps or charts to a custom dashboard

To add a map or chart to a custom dashboard:

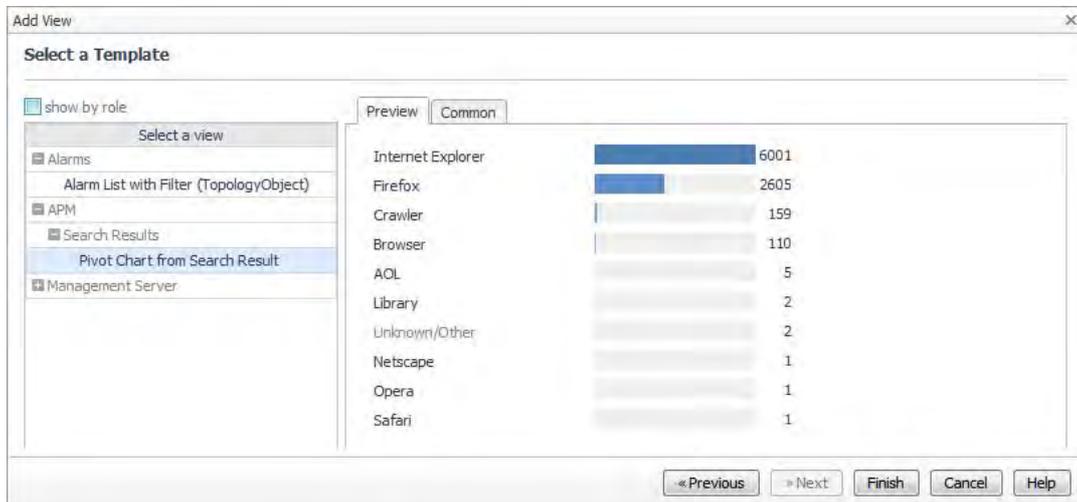
- 1 On the Map or Pivot dashboard, open the action panel and click the **General** tab.
- 2 Expand **Other Actions**.
- 3 Click **Create dashboard**.
The Create Dashboard wizard opens. To navigate between screens, use the **Next** and **Previous** buttons. For help with options, click **Help**.
- 4 On the **Build a Dashboard** screen, select **Use All Data**.
- 5 On the **View Properties** screen, specify a name for the new dashboard. Select other dashboard elements or accept the defaults.
- 6 On the **Select Dashboard Layout** screen, select a layout.
- 7 Click **Finish**.
The Add View Wizard opens automatically.
- 8 On the **Add a Dashboard View Element** screen, expand **APM > Search Results**, and then expand either **All Map Search Results** or **All Pivot Chart Search Results**. Select the map or pivot you want to add to the custom dashboard.

Figure 46. Add a Dashboard View Element screen



- 9 On the **Select a Template** screen, deselect **show by role**, and then expand **APM > Search Results**. Select the map or chart to display.

Figure 47. Select a Template screen



- 10 Click **Finish**.

The wizard creates the new dashboard with the selected view. The new dashboard is listed in the navigation panel, under **Dashboards > My Dashboards**.

- 11 To display the search results that are represented by a bar in the chart, click the bar.

Managing published maps and charts

You can view, rename, or delete maps and charts from your published Custom Dashboards list.

To view, rename, or delete a view element:

- 1 On the Map or Pivot dashboard, open the action panel and click the **General** tab.
- 2 Expand **Actions**.
- 3 Click **Manage Custom Dashboards**.
 - To view a map or chart, click its name in the list.
A window opens displaying the map or chart view element. Close the window.
 - To rename a map or chart, click its **Rename**  icon. Specify the new name, and click **Rename**.
The new view element name replaces the old name in the list.
 - To delete a map or chart, click its check box, and click **Remove**.

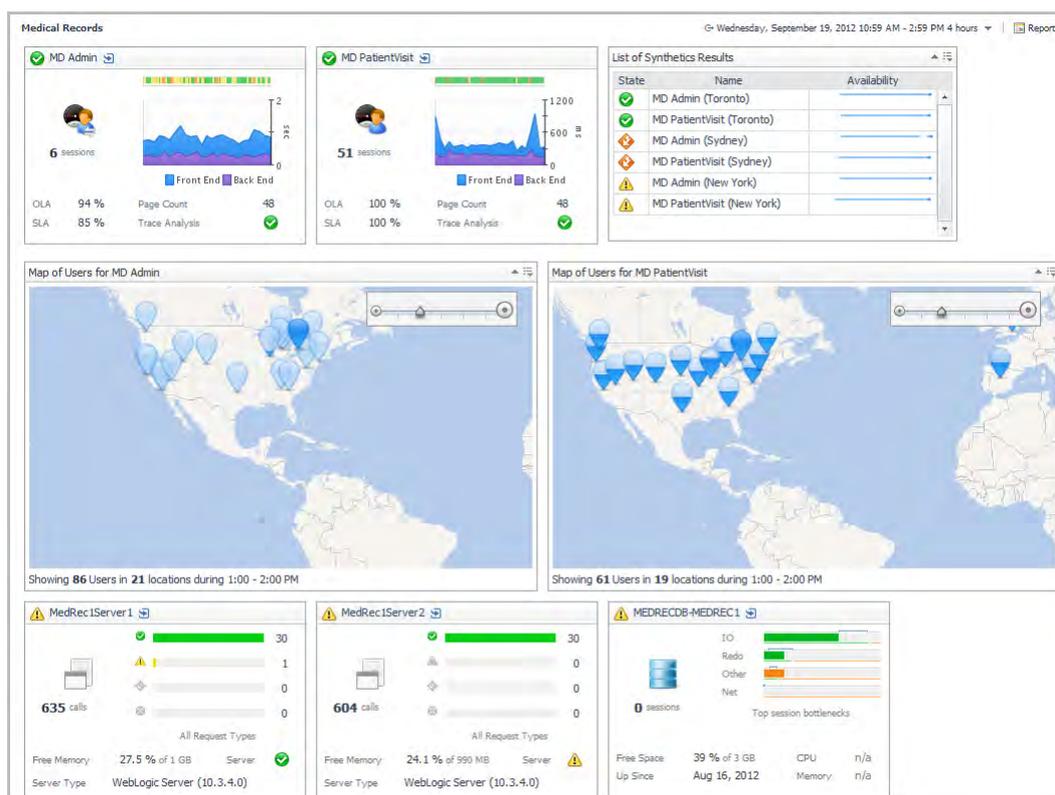
Creating custom drag-and-drop dashboards

You can quickly and easily create a drag-and-drop dashboard to customize the view you want to use for triage with a specific application. This can be helpful when you want to:

- Enhance or simplify your triage process for a specific application by exposing important components or notes for a specific application.
- Visualize your end users and applications in a geographical distribution.

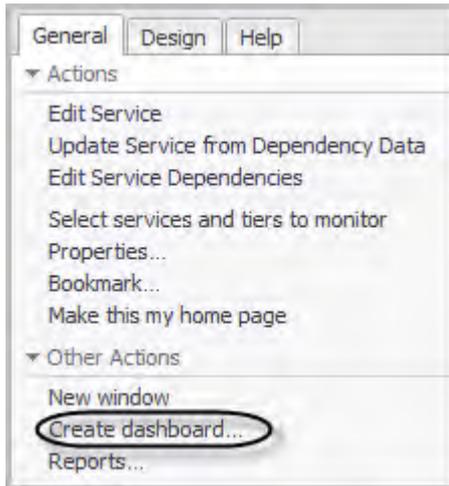
For example, suppose you have a service that includes summarized data from a number of different locations, and you want to visualize this at-a-glance, relative to their geographic location. The procedures that follow walk you through creating such a dashboard, adding view elements for Real User and Synthetic transactions, and adding map components.

Figure 48. Example of a custom dashboard created using drag-and-drop components



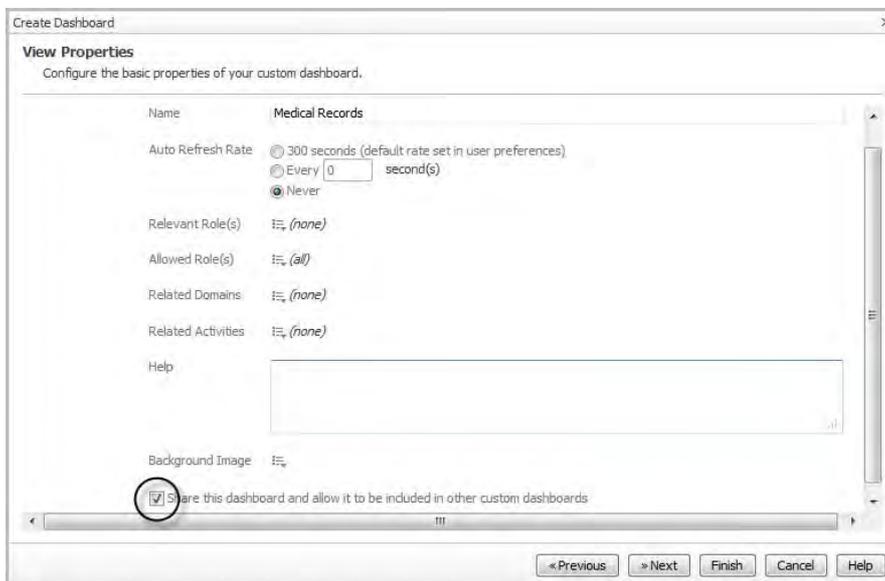
To create a custom dashboard:

- 1 Open the action panel on the right-hand side of the Foglight interface.
- 2 In the Other actions section of the action panel, click Create dashboard.



The Create Dashboard wizard opens.

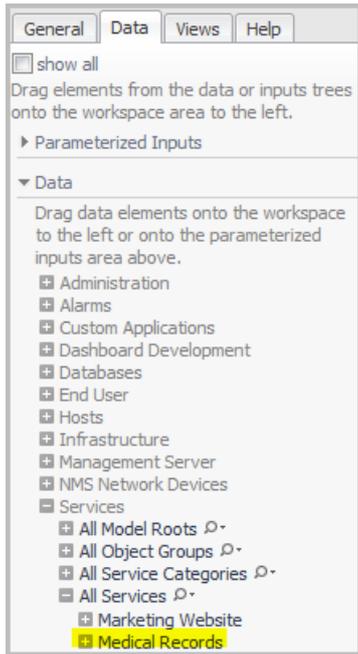
- 3 Select **Use All Data** (the default setting) and click **Next**.



- 4 On the View Properties page, type a name for your new dashboard in the **Name** box.
- 5 Select the **Share this dashboard and allow it to be included in other custom dashboards** check box.
- 6 Click **Next**.
- 7 On the Select Dashboard Layout page, select **Fixed Size**.
- 8 Click **Finish**.
- 9 The Add View wizard opens automatically. Click **Cancel**.
Next, add Real User data views to the dashboard.

To add Real User data to a custom dashboard:

- 1 On the action panel, click the **Data** tab.
- 2 In the Data list, expand **Services > All Services**.



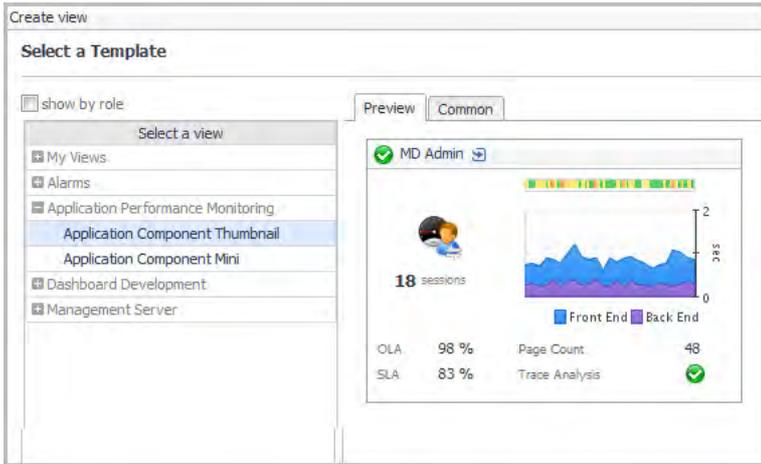
- 3 Locate and expand the service you want to view (for example, Medical Records).
- 4 Expand *Real User Results* and select the application component (for example, MD Admin).



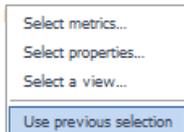
- 5 Drag and drop the application component onto the dashboard in the display area. A menu opens.



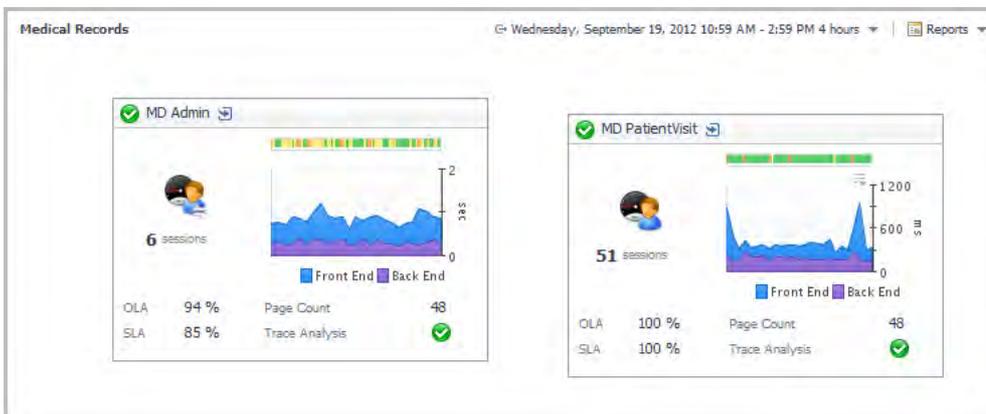
- 6 Click **Select a view**. The Create View wizard opens.
- 7 On the **Select a Template** page, expand **Application Performance Monitoring**, and click **Application Component Thumbnail**.



- 8 Click **Finish**.
- 9 Drag and drop another application component onto the dashboard (for example, MD PatientVisit).
- 10 From the menu that opens, click **Use previous selection**.



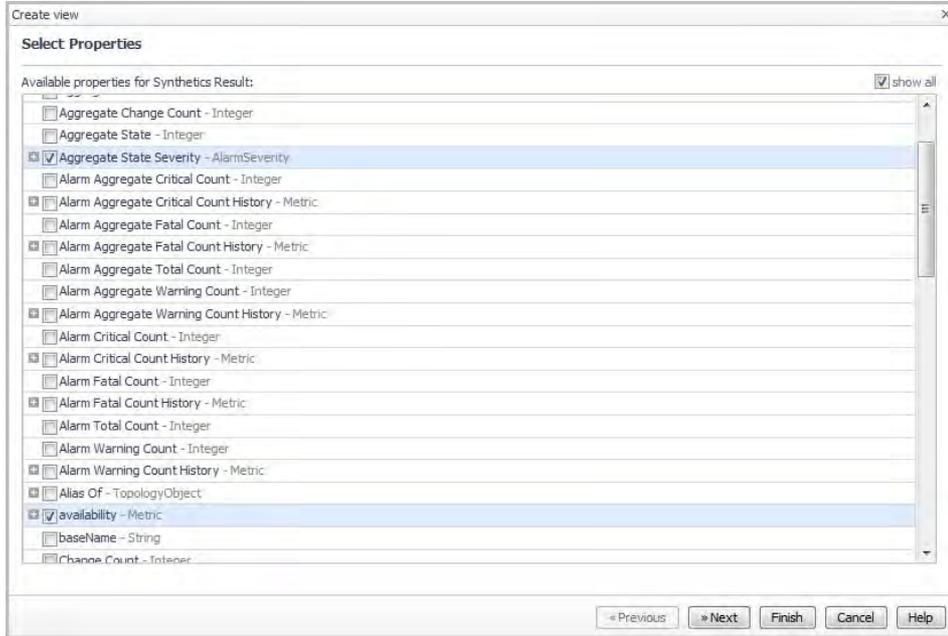
The Real User thumbnail view appears on the dashboard.



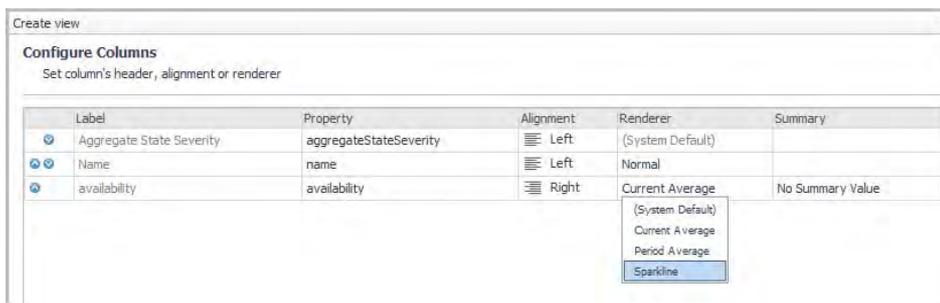
Next, add a table containing Synthetic transaction results.

To add Synthetic Transaction data to a custom dashboard.

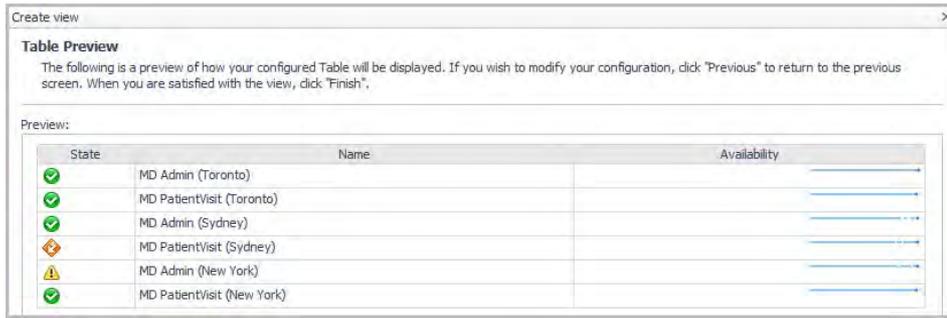
- 1 From the Data list in the action panel, drag and drop Synthetic User Results onto the dashboard display area.
- 2 From the menu that opens, select Create a table. The Create View wizard opens.
- 3 On the Select Properties page, select the Show All check box.



- 4 Select the following properties:
 - Aggregate State Severity - AlarmSeverity
 - Name - String
 - availability - Metric
- 5 Click Next.
- 6 On the Configure Columns page, click in the Renderer box for the *availability* property and select Sparkline from the list.

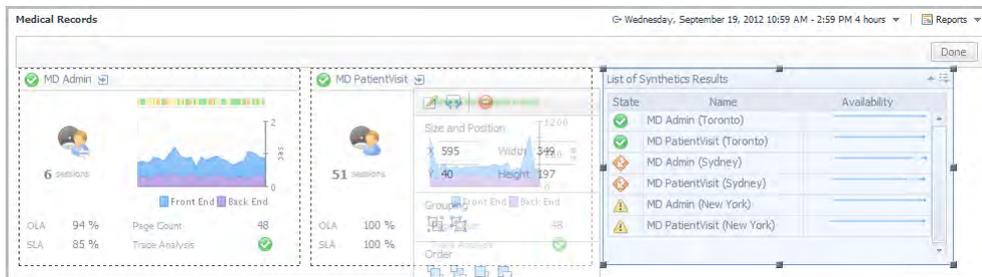


- 7 Optional – Click in the Label box for the *Aggregate State Severity* property and type State.
- 8 Optional – Click in the Label box for the *availability* property and type Availability.
- 9 Click Next.
- 10 The Table Preview page loads, displaying a preview of the table you have just configured.



If you are satisfied with the table's appearance, click **Finish**.

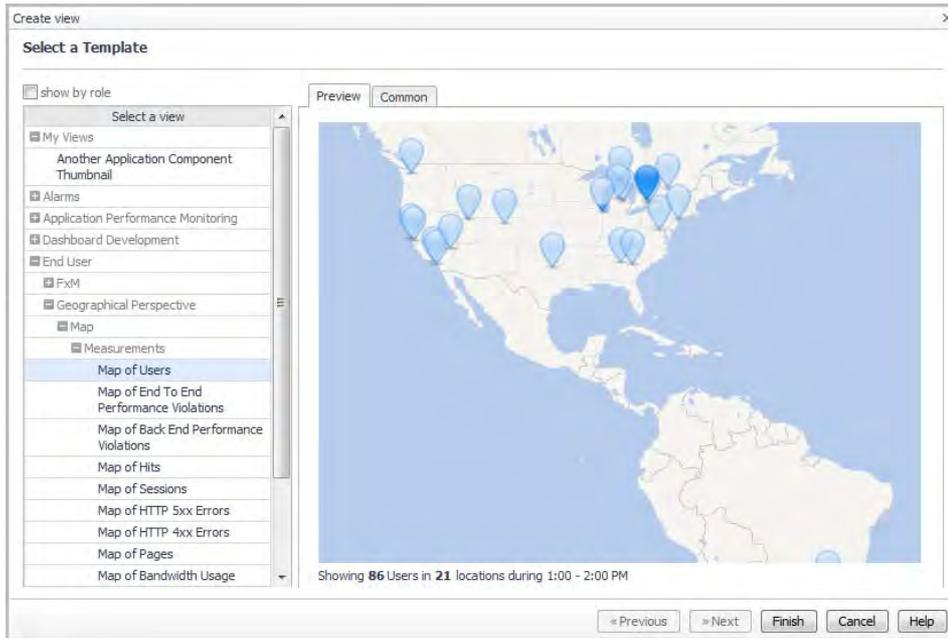
- 11 On the action panel, click the **General** tab.
- 12 Click **Edit page layout**.
- 13 Reposition the data views by dragging and dropping them into place.
- 14 With the table view selected, you can enlarge the table by dragging the border to the desired dimensions.



- 15 Click **Done** to lock the views in place and continue adding views.

To add Real User data in a Geographical Perspective to the dashboard:

- 1 On the action panel, click the **Data** tab.
- 2 Drag and drop a Real User result (for example, MD Admin) onto the dashboard.
- 3 From the menu that opens, click **Select a view**.
- 4 Expand **End User > Geographical Perspective > Measurements**.
- 5 Select **Map of Users**.



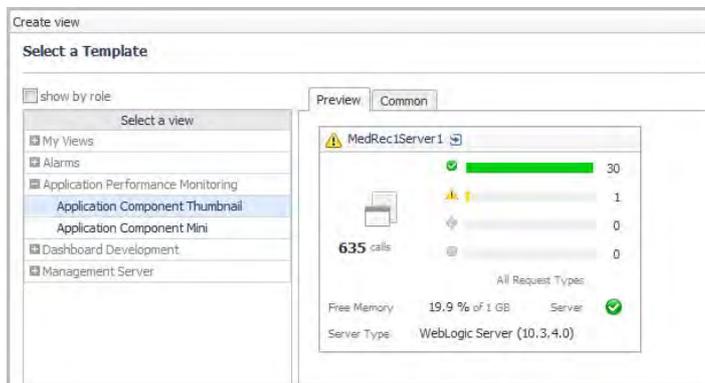
- 6 Click **Finish**.
 - 7 Drag and drop another application component onto the dashboard (for example, MD PatientVisit).
 - 8 From the menu that opens, click **Use previous selection**.
 - 9 On the action panel, click the **General** tab.
 - 10 Click **Edit page layout**.
 - 11 Reposition the data views by dragging and dropping them into place.
- Finally, add views for application and database servers.

To add application component views to the dashboard:

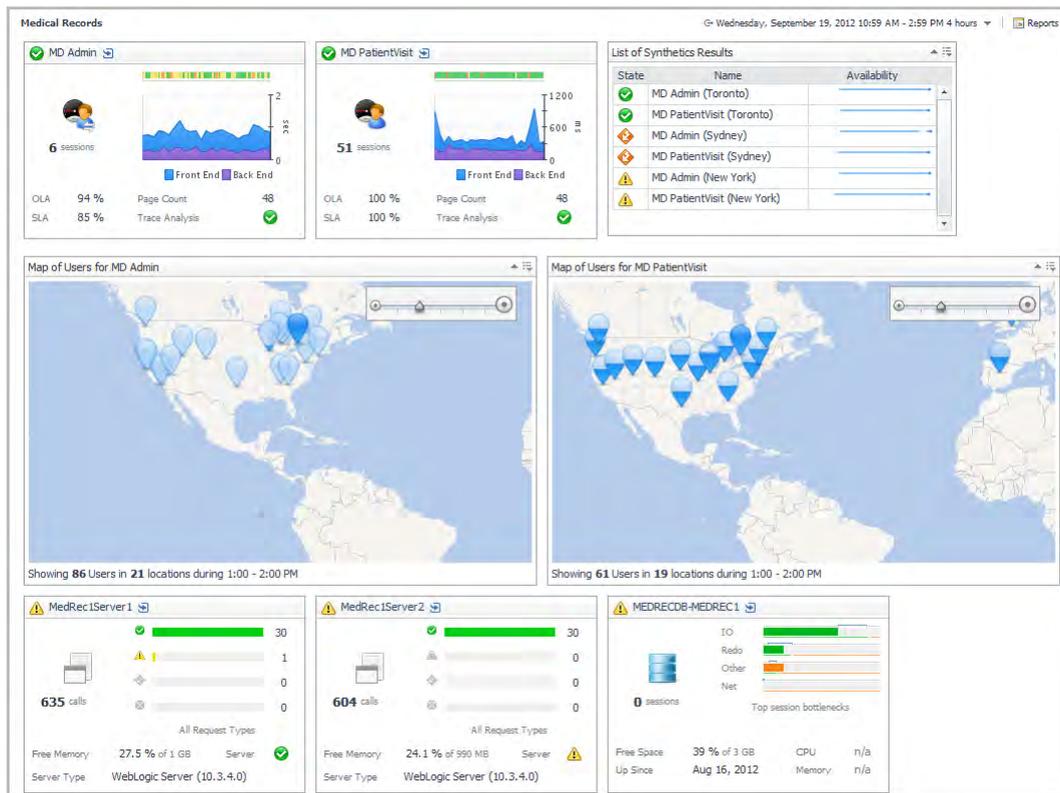
- 1 On the action panel, click the **Data** tab.



- 2 Drag and drop an application server from the **JavaEE Application Servers** list (for example, **MedRec1Server1**).
- 3 On the menu that opens, click **Select a view**.
- 4 Expand **Application Performance Monitoring** and click **Application Component Thumbnail**.



- 5 Click **Finish**.
- 6 Drag and drop another application server onto the dashboard (for example, **MedRec1Server2**).
- 7 On the menu that opens, click **Use previous selection**.
- 8 Reposition the thumbnail views as necessary.
- 9 Expand **Oracle Instances** and drag and drop a database server instance onto the dashboard (for example, **MEDRECDB-MEDRECT**).
- 10 On the menu that opens, click **Select a view**.
- 11 Expand **Application Performance Monitoring** and click **Application Component Thumbnail**.
- 12 Click **Finish**.
- 13 On the action panel, click the **General** tab.
- 14 On the dashboard, click **Done**.



The at-a-glance custom dashboard is now complete.

You can link this dashboard to the Explore icon for the service it represents on the Service Operations Console. For more information, see [Linking a custom dashboard to the Explore icon for a service](#).

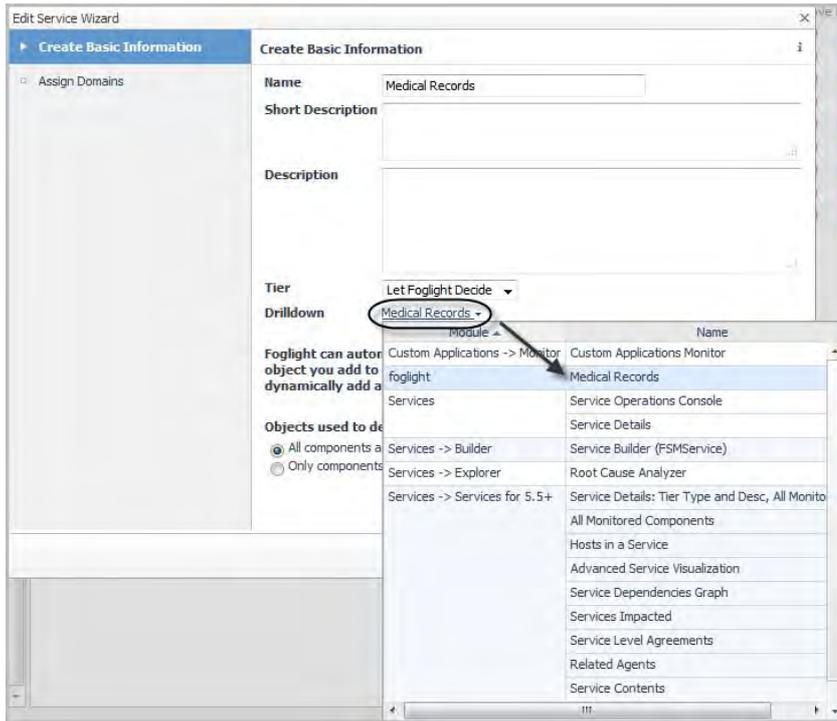
Linking a custom dashboard to the Explore icon for a service

After you have created the dashboard, you can add a link to it from the Explore icon for a service in the SOC.

NOTE: This feature requires Foglight Management Server 5.6.4 or later.

To link a custom dashboard to the SOC:

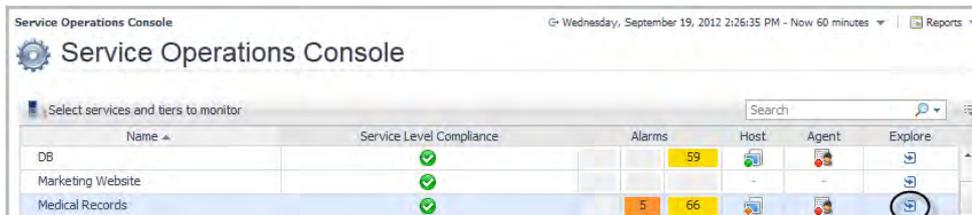
- 1 Open the Service Builder. Under **Dashboards**, click **Services > Service Builder**.
- 2 Locate the service in the Component list (for example, Medical Records).
- 3 Click the edit icon  for the tier. The Edit Service Wizard opens.
- 4 On the Create Basic Information page, click the text link beside **Drilldown**. A list opens.



- 5 Locate the custom dashboard to which you want to link.
- 6 Click the name of the dashboard.
The list closes, and the name appears on the Create Basic Information page.
- 7 Click Finish.

Now, return to the SOC and click the Explore icon  for the service.

Figure 49. Service Operations Console dashboard



The custom dashboard opens.

For more information about creating custom dashboards, see the *Foglight User Help*.

APM tile and view reference

This section contains reference information about APM-related tiles and views. Read this section to find out more details about the metrics appearing on these views.

Foglight displays monitoring data in views that group, format, and display data. The main types are described here.

Dashboards are top-level views that contain lower-level views. The dashboards supplied with Foglight, as well as those created by users, are accessible from the navigation panel.

Lower-level views in Foglight can be added to dashboards or can be accessed by drilling down from a dashboard. They receive and display data directly from the Management Server or from other views. Some views filter or select data that appears in other views in the same dashboard. Some are tree views with expandable nodes for selecting servers, applications, or data.

NOTE: If you build services for the SOC using the traditional Service Builder in Foglight (Dashboards > Services > Service Builder), you must manually identify and select the appropriate topology objects. The topology object names are provided here, below the image of the associated tile.

For a general introduction to the APM tiles and detail views, see [Overview of APM tiles](#) and [Overview of Detail views](#).

The following table includes a list of monitored domain icons and links to their matching tile views.

Table 22. Monitored domain tiles

Tile Icon	Tile Name
	Application Servers - .NET tile Application Servers - Java tile
	DB2 tile
	Host tile
	JMX tile
	MQ tile
	Oracle tile
	OS tiles <ul style="list-style-type: none"> • Server - Apache Monitor tile • Application Monitor tile • Log Filter tile • Web Monitor tile

Table 22. Monitored domain tiles

	Pivot tiles
	Real User (APM) tile
	Real User (FxM) tile
	Sequence tile
	SQL Server tile
	Sybase tile
	Synthetics tile <ul style="list-style-type: none"> • Multi-Location Synthetics tile • Single-Location Synthetics tile
	Virtual Hyper-V tile
	VMware tile

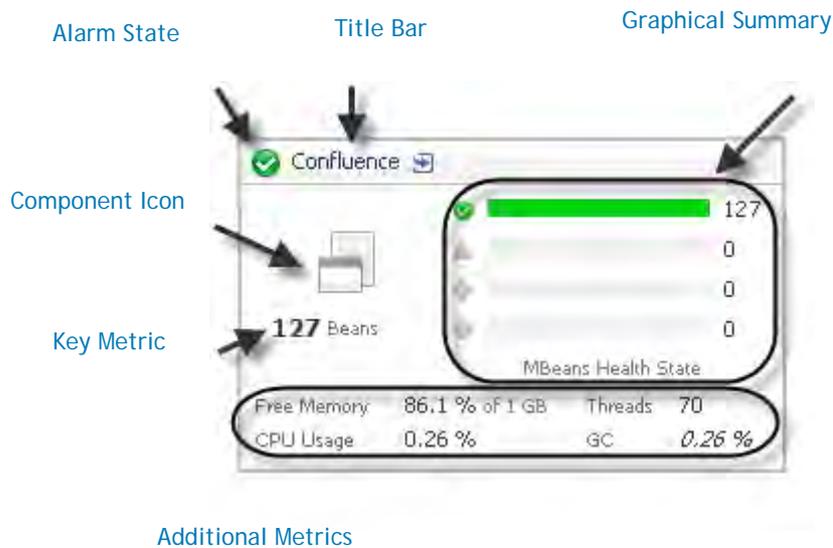
For a list of topology object names associated with these tiles, see [Topology object name reference table](#).

Overview of APM tiles

Foglight APM includes a tile view for each monitored domain. In order to populate these tiles, the appropriate Foglight cartridge must be installed and configured to monitor the domain or component. For example, in order to view the [Application Servers - Java tile](#), you must install Foglight for Java EE Technologies and configure it to monitor at least one Java™ application server.

The metrics displayed on a tile are specific to the domain, but the overall look and functionality of the tiles are common. For example, the following tile presents JMX data:

Figure 50. An example of a JMX Server domain tile



Topology Object Name: JMXServer

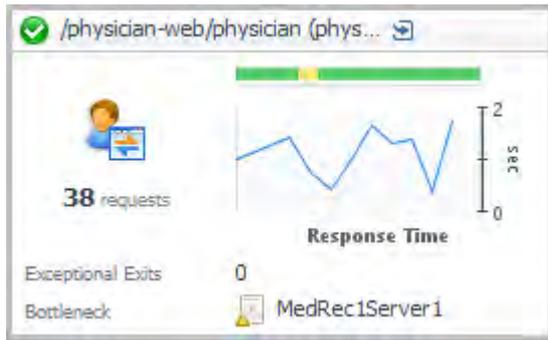
Table 23. Example descriptions of the JMX Server domain example tile

Alarm State	The icon in the top left corner indicates the current state of alarms for the component.
Title Bar	The title bar includes the component name, and the Explore icon  . Click the icon to open a detail view. For more information, see Overview of Detail views .
Component Icon	Each component is represented by a unique icon that provides easy, at-a-glance recognition of the domain.
Key Metric	The most important metric for the domain is displayed in the largest font, directly below the component icon, on the left side of the tile. Where no one metric takes precedence (for example, on the Host tile), the current alarms are displayed instead.
Graphical Summary	The right side of the tile displays a graphical summary of key metrics for the component. For example, the JMX tile includes a health breakdown for MBeans, as in the example above. Other domains include a chart of the key metric for the time range selected (such as Response Time), an overall health history (color-coded bar), or a list of session bottlenecks.
Additional Metrics	Additional metrics that are key to the component appear at the bottom of the tile. NOTE: The values of these metrics are always current, unless the value appears in italics (for example, GC <i>0.26%</i>). Italicized metrics reflect the period average instead of the current value.

Application Servers - .NET tile

Use the Application Servers - .NET tile to gather performance information about the state of .NET[®] transactions monitored by Foglight for Microsoft .NET, version 5.9.x or later.

Figure 51. Example of the Foglight for Microsoft .NET tile view



Topology Object Name: CustomApplicationTransaction

Table 24. Description of the Foglight for Microsoft .NET view

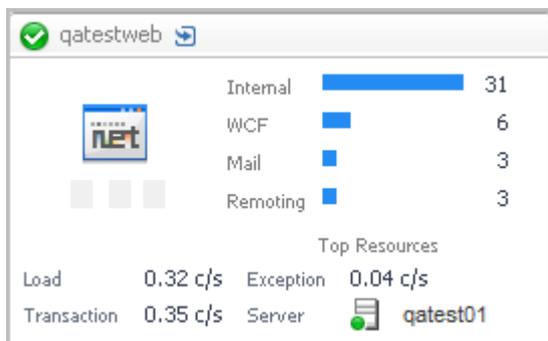
Data displayed	
	<ul style="list-style-type: none"> • Hits. The number of calls served in the most recent collection interval.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> • Response Time. A plot of the request response time.
	<ul style="list-style-type: none"> • Exceptional Exits. The number of exceptional exits recorded.
	<ul style="list-style-type: none"> • Bottleneck. Indicates the portion of the application where requests are experiencing slowdowns.

NOTE: The Foglight application server monitoring solutions, Foglight for Microsoft .NET and Foglight for Java EE Technologies, share a single tile view as of version 5.9.1. For older versions of the Cartridge for Microsoft .NET, see the [.NET tile](#).

.NET tile

Use the .NET tile to gather performance information about the state of .NET® transactions monitored by Foglight for Microsoft .NET, version 5.6.x or earlier.

Figure 52. Example of the .NET legacy tile view



Topology Object Name: NETApplicationInstance

This tile displays the current top used external resources from the list below.

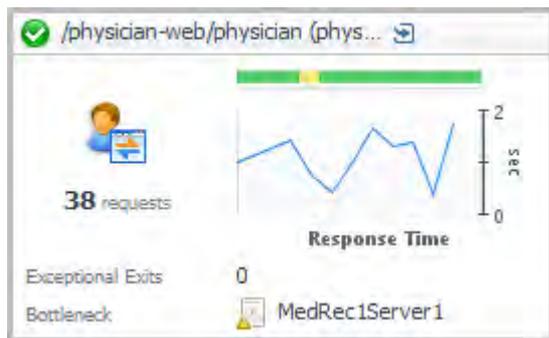
Table 25. Description of the legacy .NET tile view

Data displayed	Alarms. A count of fatal, critical, and warning alarms on the host system.
	<p>The four top used external resources from the following list are displayed on the tile:</p> <ul style="list-style-type: none"> • Internal. All method calls that are not related to any other call types in this list. • Database. Method calls related to databases. • Web Svc. Method calls related to web services. • Mail. Method calls related to sending mail. • Remoting. Method calls related to remoting client-side resources. • WCF. Method calls related to WCF client-side resources.
	<ul style="list-style-type: none"> • Load. The average load on the .NET[®] system. • Transaction. The current number of transactions per second. • Exception. The current number of exceptions per second. • Server. The .NET server name.

Application Servers - Java tile

The Application Servers - Java Tile summarizes the performance of a Java EE system monitored by Foglight for Java EE Technologies. Use this tile to gather performance information about the state of Java™ transactions.

Figure 53. Example of the Java tile view



Topology Object Name: CustomApplicationTransaction

NOTE: In previous releases, the topology object for the Cartridge for Java EE Technologies was `JavaEEAppServer`.

If the application server includes Request Types in the selected time range and the server has served at least one request in the selected time range, you can click the title bar to drill down to the [Application Server detail view](#). If there are no request types, clicking the title bar drills down to the server details.

Table 26. Description of the Foglight for Java tile view

Data displayed	<ul style="list-style-type: none"> • Hits. The number of calls served in the most recent collection interval.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> • Response Time. A plot of the request response time.

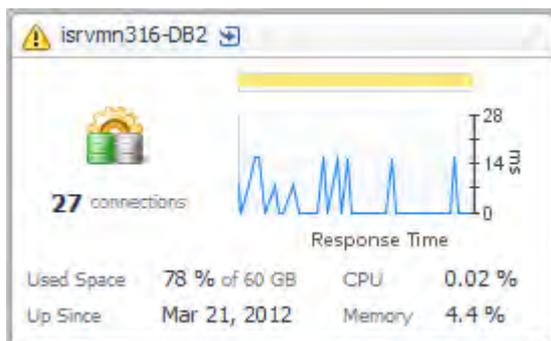
Table 26. Description of the Foglight for Java tile view

- **Exceptional Exits.** The number of exceptional exits recorded.
- **Bottleneck.** Indicates the portion of the application where requests are experiencing slowdowns.

DB2 tile

Use the DB2 tile to gather performance information about the state of DB2 transactions monitored by Foglight for DB2 LUW.

Figure 54. Example of the DB2 tile view



Topology Object Name: DB2_Instance

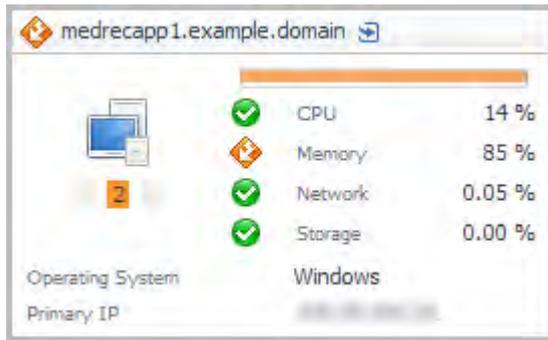
Table 27. Description of the DB2 tile view

Data displayed	<ul style="list-style-type: none"> • Number of Connections. The sum of the average number of local and remote DB2 connections.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> • Response Time. A plot of the database response time.
	<ul style="list-style-type: none"> • Used Space. The average amount of database space used, as a percentage of the total space available.
	<ul style="list-style-type: none"> • Up Since. The date the database was last restarted.
	<ul style="list-style-type: none"> • CPU. The average CPU usage for all DB2 agents.
	<ul style="list-style-type: none"> • Memory. The average memory usage for all DB2 agents.

Host tile

The Host Tile summarizes the performance of a host system monitored by Foglight for Infrastructure. Use this tile to gather performance information about the state of host transactions.

Figure 55. Example of the Host tile view



You can click the title bar to drill down to the [Host detail view](#).

Topology Object Name: Host

NOTE: For hosts, always select the host object, regardless of whether or not the host is virtual (for example, Hyper-V® or VMware®). Foglight looks for the appropriate host extensions and displays the associated host dashboard (physical or virtual).

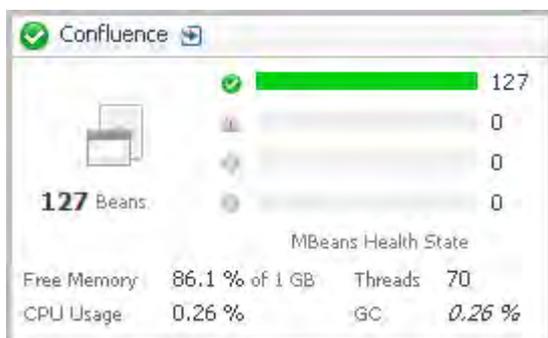
Table 28. Description of the Host tile view

Data displayed	Description
Alarms	A count of fatal, critical, and warning alarms on the host system.
CPU	An icon representing the health state of the CPU, and the CPU utilization expressed as a percentage of the total available.
Memory	An icon representing the health state of the memory, and the memory utilization expressed as a percentage of the total available.
Network	An icon representing the health state of the network transactions, and the network utilization expressed as a percentage of the total available.
Storage	An icon representing the health state of the storage (disk space), and the disk utilization expressed as a percentage of the total available.
Operating System	The name of the operating system.
Primary IP	The primary IP address for the host system.

JMX tile

The JMX Tile summarizes the performance of a JMX Server system monitored by the Cartridge for JMX. Use this tile to gather performance information about the state of JMX MBean transactions.

Figure 56. Example of the JMX tile view



Topology Object Name: JMXServer

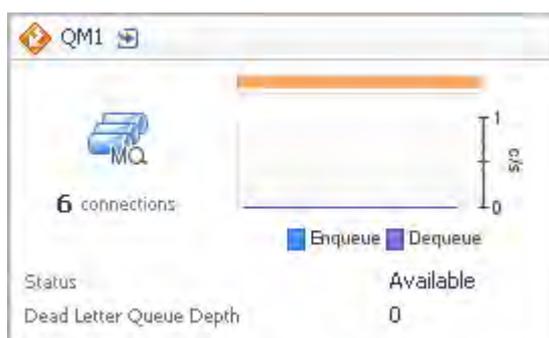
Table 29. Description of the JMX tile view

Data displayed	<ul style="list-style-type: none"> • MBeans. The current average number of MBeans. • MBean Health Breakdown. The current number of MBeans in each state (Normal , Warning , Critical , Fatal ) , along with a color-coded bar. The length of colored bar indicates the number of MBeans in the corresponding state compared to the total number of MBeans. • Free Memory. The current free JVM memory, expressed as a percentage of the total allocated. • CPU Usage. The current average CPU usage. • Threads. The current number of threads. • GC. The period average garbage collection overhead expressed as a percentage for the selected time range.
----------------	--

MQ tile

Use the MQ Tile to gather performance information about the state of queue transactions on an MQ Queue Manager monitored by the Foglight *for IBM WebSphere MQ Server*.

Figure 57. Example of the MQ tile view



Topology Object Name: MQQueueManager

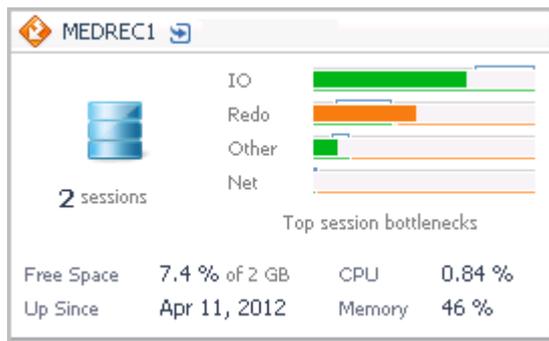
Table 30. Description of the MQ tile view

Data displayed	<ul style="list-style-type: none"> • Number of Connections. The average number of queue manager connections. • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state. • Enqueue/Dequeue. The plotted message enqueue and dequeue rates. • Status. The average queue status for the time range: available, unavailable, or unknown. • Dead Letter Queue Depth. The average depth of the dead letter (undeliverable messages) queue.
----------------	--

Oracle tile

Use the Oracle Tile to gather performance information about the state of Oracle® database transactions monitored by Foglight for Oracle. This tile displays the current top used resources from the list below.

Figure 58. Example of the Oracle tile view



Topology Object Name: DBO_Instance

Table 31. Description of the Oracle tile view

Data displayed	<ul style="list-style-type: none"> • Sessions. The current average number of active sessions.
	<p>Top Session Bottlenecks. A breakdown of the health state of potential session bottleneck points by severity. The four top used resources from the list below are displayed on the tile.</p> <ul style="list-style-type: none"> • IO • Network • Buffer • Lock • Latch • Redo • Cluster • CPU Usage • CPU Wait • Other
	<ul style="list-style-type: none"> • Free Space. The amount of database storage space available, expressed as a percentage of the total available.
	<ul style="list-style-type: none"> • Up Since. The date the database was last restarted.
	<ul style="list-style-type: none"> • CPU. The average CPU usage for all Oracle® agents.
	<ul style="list-style-type: none"> • Memory. The average memory usage for all Oracle agents.

OS tiles

Use the OS Tiles to gather performance information about the state of Apache servers, application server hosts, Log Filter agents, or web servers. The OS Tiles require the Cartridge for Operating Systems.

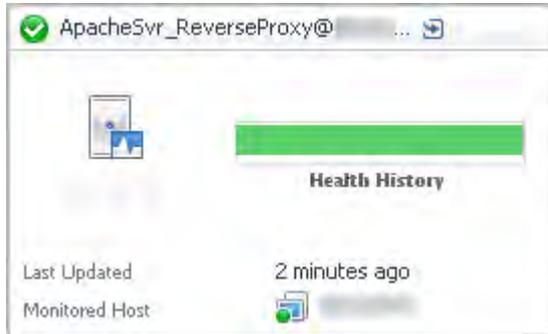
For more information, see the following topics:

- [Server - Apache Monitor tile](#)
- [Application Monitor tile](#)
- [Log Filter tile](#)
- [Web Monitor tile](#)

Server - Apache Monitor tile

The Apache Monitor Tile summarizes the performance of an Apache server. Use this tile to gather performance information about the state of Apache server transactions.

Figure 59. Example of the Server - Apache Monitor tile view



Topology Object Name: ApacheSvrAgent

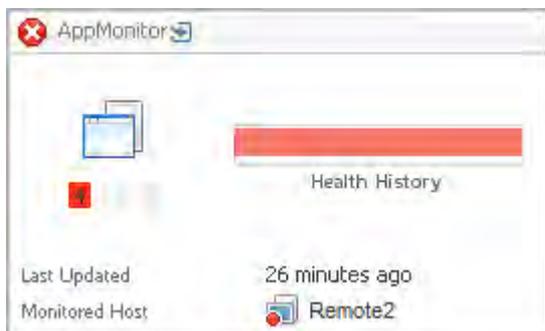
Table 32. Description of the Server - Apache Monitor tile view

Data displayed	<ul style="list-style-type: none">• Alarms. A count of fatal, critical, and warning alarms on the host system.• Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.• Last Updated. The amount of time, in minutes, since the host information was last updated.• Monitored Host. The name of the monitored host, and an icon representing the type of host.
-----------------------	---

Application Monitor tile

The Application Monitor Tile summarizes the performance of an application server. Use this tile to gather performance information about the state of server transactions.

Figure 60. Example of the Application Monitor tile view



Topology Object Name: AppMonitorAgent

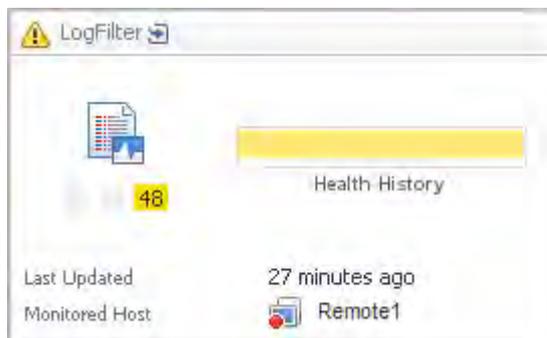
Table 33. Description of the Application Monitor tile view

Data displayed	<ul style="list-style-type: none"> • Alarms. A count of fatal, critical, and warning alarms on the host system.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> • Last Updated. The amount of time, in minutes, since the host information was updated.
	<ul style="list-style-type: none"> • Monitored Host. The name of the monitored host, and an icon representing the type of host.

Log Filter tile

The Log Filter Tile summarizes the performance of an Alarm Filter agent. Use this tile to gather performance information about the state of log filter transactions.

Figure 61. Example of the LogFilter tile view



Topology Object Name: LogFilterAgent

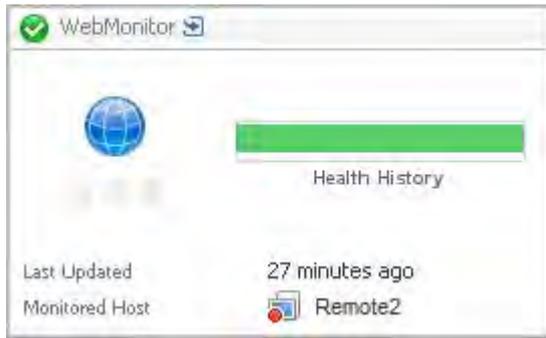
Table 34. Description of the LogFilter tile view

Data displayed	<ul style="list-style-type: none"> • Alarms. A count of fatal, critical, and warning alarms on the host system.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> • Last Updated. The amount of time, in minutes, since the host information was last updated.
	<ul style="list-style-type: none"> • Monitored Host. The name of the monitored host, and an icon representing the type of host.

Web Monitor tile

The Web Monitor Tile summarizes the performance of a web server. Use this tile to gather performance information about the state of server transactions.

Figure 62. Example of the Web Monitor tile view



Topology Object Name: WebMonitorAgent

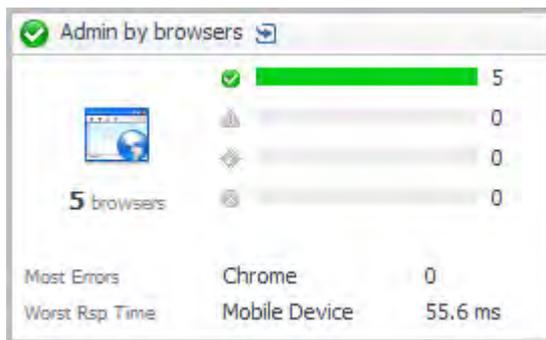
Table 35. Description of the Web Monitor tile view

Data displayed	<ul style="list-style-type: none"> • Alarms. A count of fatal, critical, and warning alarms on the host system.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> • Last Updated. The amount of time, in minutes, since the host information was last updated.
	<ul style="list-style-type: none"> • Monitored Host. The name of the monitored host, and an icon representing the type of host.

Pivot tiles

The Pivot tiles display metrics from pivots defined in Foglight APM analyzers. The layout of the tiles is common, with a unique icon representing one of four types of pivot groups: browsers, content types, locations, and OSes.

Figure 63. Example of a Pivot tile view



You can click the title bar to drill down to [Pivot Breakdown detail view](#).

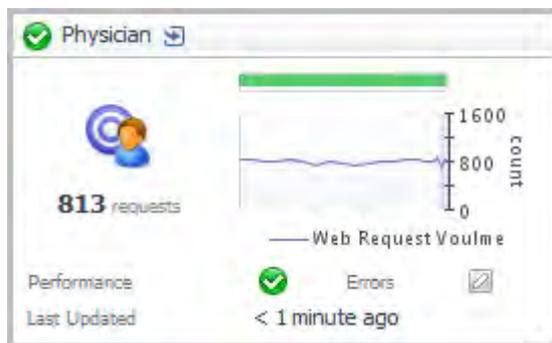
Table 36. Description of the Pivot tiles view

	<ul style="list-style-type: none"> • Icon. Indicates the type of pivots.
	<ul style="list-style-type: none"> •  – Content type pivots.
	<ul style="list-style-type: none"> •  – Endpoint pivots.
Data displayed	<ul style="list-style-type: none"> •  – Location pivots.
	<ul style="list-style-type: none"> •  – OS pivots.
	<ul style="list-style-type: none"> •  – Web browser pivots.
	<ul style="list-style-type: none"> • Health Breakdown. The current number of pivots in each state (Normal , Warning , Critical , Fatal ) along with a color-coded bar. The length of colored bar indicates the number of pivots in the corresponding state compared to the total number of pivots.
	<ul style="list-style-type: none"> • Most Errors. The pivot type with the most errors. For example, for web browser pivots, this may be Chrome™, Firefox®, Internet Explorer®, Opera™, or Mobile Device. For a location pivot, this metric would indicate the city and country.
	<ul style="list-style-type: none"> • Worst Response Time. The pivot type with the longest response time.

Real User (APM) tile

The Real User (APM) tile shows summarized data about real user transactions captured by Foglight APM analyzers.

Figure 64. Example of the Real User (APM) tile view



Topology Object Name: EUHitInteraction

Click the title bar to drill down to the [Real User \(APM\) Performance detail view](#).

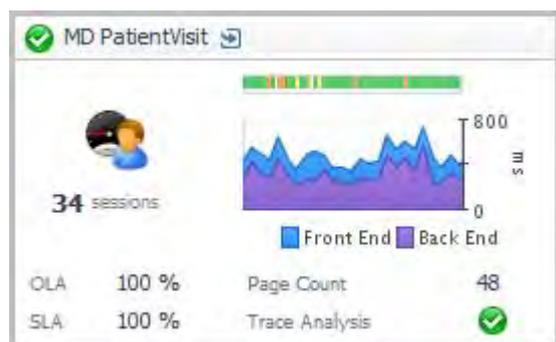
Table 37. Description of the Real User (APM) tile view

Data displayed	<ul style="list-style-type: none"> • Requests. The total number of requests for the transaction.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> • Web Request Volume (count). A graph of the number of web requests over time.
	<ul style="list-style-type: none"> • Performance. This indicator shows that performance metrics are tracking to their historical norms. Deviations from those norms indicate an anomaly that should be investigated.
	<ul style="list-style-type: none"> • Errors. This indicator shows that errors are tracking to their historical norms. Deviations from those norms indicate an anomaly that should be investigated.
	<ul style="list-style-type: none"> • Last Updated. The time the metrics were last updated for this transaction.

Real User (FxM) tile

The Real User (FxM) tile shows summarized data about real user transactions captured by Foglight Experience Monitor (FxM).

Figure 65. Example of the Real User (FxM) tile view



Topology Object Name: FxMApplicationResult

Click the title bar to drill down to the [Real User \(FxM\) Performance detail view](#).

Table 38. Description of the Real User (FxM) tile view

Data displayed	<ul style="list-style-type: none"> • Current Sessions. The total number of active end users that are currently interacting with the monitored transaction.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> • Front End. The time from when the first byte of a transaction is sent from the end user's browser until the time the last byte of that transaction was processed in the browser. This includes all Back End time, network time, and browser processing time. Front End times are given over the time range period selected in the SOC.
	<ul style="list-style-type: none"> • Back End. The time from when the first byte of a transaction request is detected on the receiving web server until the time the last byte of that transaction response was sent out of the web server. This includes all web server time, application server time, database time, and web service call time spent behind the web server needed to fulfill the transaction request. Back End times are given over the time range selected.

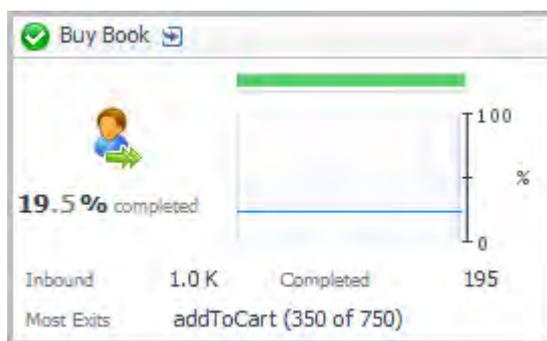
Table 38. Description of the Real User (FxM) tile view

<ul style="list-style-type: none"> OLA. The current average percentage of pages that satisfy the Operation Level Agreement (OLA), as defined by the Page Processing Time threshold.
<ul style="list-style-type: none"> SLA. The current average percentage of pages that satisfy the Service Level Agreement (SLA), as defined by the Page End-to-End Time threshold.
<ul style="list-style-type: none"> Page Count. The average number of page download requests over the time range selected.
<ul style="list-style-type: none"> Trace Analysis. If any counters are selected in the Real User (FxM) Performance detail view, this indicator shows the highest severity alarm raised against one or more selected counters: Normal , Warning , Critical , or Fatal . If no counters are selected, this indicator appears disabled . This indicator shows that trace analysis metrics are tracking to their historical norms. Deviations from those norms indicate an anomaly that should be investigated.

Sequence tile

Use the Sequence Tile to review a summary of a sequence defined by a Foglight APM sequence analyzer.

Figure 66. Example of the Sequence tile view



Topology Object Name: `EUSequenceInteraction`

Click the title bar to open the Sequences dashboard.

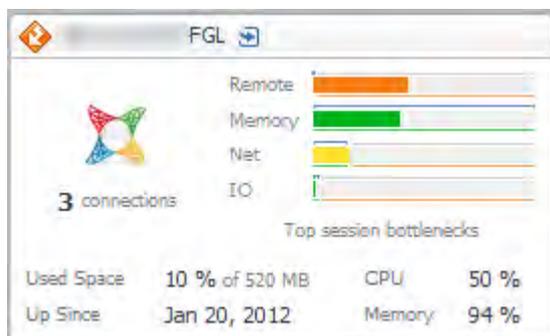
Table 39. Description of the Sequence tile view

<p>Data displayed</p>	<ul style="list-style-type: none"> Percent Completed. Summarizes the number of successful completions of the sequence as a percentage of total sequences initiated. The graph presents the same data.
	<ul style="list-style-type: none"> Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> Inbound. The number of hits on the first event in the sequence.
	<ul style="list-style-type: none"> Completed. The number of successfully completed sequences.
	<ul style="list-style-type: none"> Most Exits. The event in the sequence with the largest number of exits. Both the name of the event and the number of exits out of the total hits are displayed.

SQL Server tile

Use the SQL Server Tile to gather performance information about the state of SQL Server® database transactions monitored by Foglight for SQL Server. This tile displays the current top used resources from the list below.

Figure 67. Example of the SQL Server tile view



Topology Object Name: DBSS_Instance

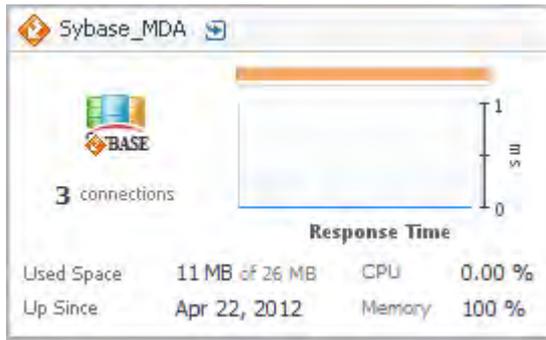
Table 40. Description of the SQL Server tile view

Data displayed	
	<ul style="list-style-type: none">• Connections. The current average number of active connections.
	<ul style="list-style-type: none">• Top Session Bottlenecks. A breakdown of the potential session bottleneck points. The four top used resources from the list below are displayed on the tile.
	<ul style="list-style-type: none">• IO• Lock• Latch• Network• CPU• CPU Usage• Memory• CLR• Log• Remote Provider• Other
	<ul style="list-style-type: none">• Used Space. The amount of database storage space used, expressed as a percentage of the total available.
	<ul style="list-style-type: none">• Up Since. The date the database was last restarted.
	<ul style="list-style-type: none">• CPU. The average CPU usage for all SQL Server® agents.
	<ul style="list-style-type: none">• Memory. The average memory usage for all SQL Server agents.

Sybase tile

Use the Sybase Tile to gather performance information about the state of Sybase® database transactions monitored by Foglight for Sybase.

Figure 68. Example of the Sybase tile view



Topology Object Name: Sybase_MDAAgent

Table 41. Description of the Sybase tile view

Data displayed	Description
	<ul style="list-style-type: none"> • Connections. The current average number of active connections.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> • Response Time. The time elapsed during database access, plotted over time.
	<ul style="list-style-type: none"> • Used Space. The amount of database storage space used, expressed as a percentage of the total available.
	<ul style="list-style-type: none"> • Up Since. The date the database was last restarted.
	<ul style="list-style-type: none"> • CPU. The average CPU usage for all Sybase® agents.
	<ul style="list-style-type: none"> • Memory. The average memory usage for all Sybase agents.

Synthetics tile

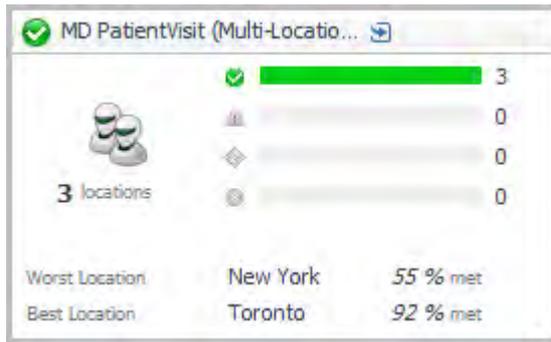
The Multi-Location and Single-Location Synthetics Tiles tile show summarized data about user transactions captured by Foglight Transaction Recorder (FTR):

- [Multi-Location Synthetics tile](#)
- [Single-Location Synthetics tile](#)

Multi-Location Synthetics tile

The Multi-Location Synthetics Tiles summarizes the performance of a synthetic transaction from multiple locations. Use this tile to gather performance information about the overall state of rolled up locations.

Figure 69. Example of the Multi-Location Synthetics tile view



Topology Object Name: FTRResult

Click the title bar to drill down to the [Synthetic User Performance detail view](#).

Table 42. Description of the Multi-Location Synthetics tile view

Data displayed	<ul style="list-style-type: none"> • Locations. The current number of agent locations.
	<ul style="list-style-type: none"> • Location Health Breakdown. The current number of locations in each state (Normal , Warning , Critical , Fatal ) , along with a color-coded bar. The length of colored bar indicates the number of locations in the corresponding state compared to the total number of locations.
	<ul style="list-style-type: none"> • Worst Location. The location of the Foglight APM Transaction Player Intelligent Agent with the worst period average success rates.
	<ul style="list-style-type: none"> • Best Location. The location of the Foglight APM Transaction Player Intelligent Agent with the best period average success rates.

NOTE: Best and Worst Location are always displayed, even when all locations are 100% operational.

Single-Location Synthetics tile

The Single-Location Synthetics tile displays a summary of a synthetic transaction from a single location.

Figure 70. Example of the Single-Location Synthetics tile view



Click the title bar to drill down to the [Synthetic Result detail view](#).

Table 43. Description of the Single-Location Synthetics tile view

Data displayed	<ul style="list-style-type: none"> • Executions. The number of times the script executed over the time range selected.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> • Response Time. The average script execution time over the time range selected. The red dashed line indicates the response time threshold. The background shading of the chart represents the status. Green shading indicates that the response time is currently good.
	<ul style="list-style-type: none"> • Availability. The period average percentage of time the service is available.
	<ul style="list-style-type: none"> • Met. The period average percentage of time the service met its required Service Level Agreement for the expected response time.
	<ul style="list-style-type: none"> • Latest. The most recent time the script executed.
	<ul style="list-style-type: none"> • Agent Status. An icon indicating the current state of the FTR agent: Normal 🟢, Warning 🟡, Critical 🟠, or Fatal 🔴.

Virtual Hyper-V tile

Use the Hyper-V Tile to gather performance information about the state of virtual Hyper-V[®] transactions monitored by the Foglight for Hyper-V.

Figure 71. Example of the Virtual Hyper-V tile view



Topology Object Name: Host

NOTE: For hosts, always select the host object, regardless of whether or not the host is virtual (for example, Hyper-V[®] or VMware[®]). Foglight looks for the appropriate host extensions and displays the associated host dashboard (physical or virtual).

Table 44. Description of the Virtual Hyper-V tile view

Data displayed	<ul style="list-style-type: none"> • Alarms. A count of fatal, critical, and warning alarms on the virtual Hyper-V[®] instance.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.

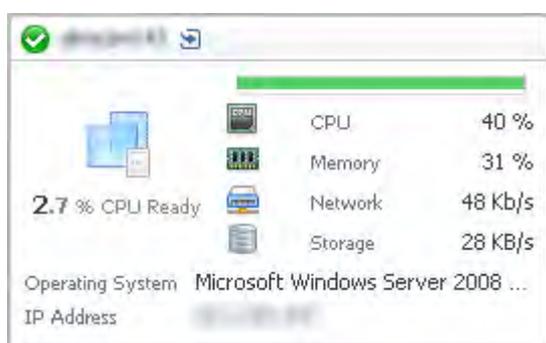
Table 44. Description of the Virtual Hyper-V tile view

• CPU. The average CPU usage for the virtual system.
• Network. The average network transfer rate for the virtual machine.
• Storage. The average disk transfer rate for the virtual machine.
• Operating System. The name of the operating system.
• IP Address. The primary IP address for the virtual machine.

VMware tile

Use the VMware Tile to gather performance information about the state of a virtual machine monitored by the Foglight for VMware.

Figure 72. Example of the VMware tile view



Topology Object Name: Host

NOTE: For hosts, always select the host object, regardless of whether or not the host is virtual (for example, Hyper-V® or VMware®). Foglight looks for the appropriate host extensions and displays the associated host dashboard (physical or virtual).

Click the title bar to drill down to the [Virtual Machine detail view](#).

Table 45. Description of the VMware tile view

Data displayed	<ul style="list-style-type: none"> • CPU Ready. The percentage of time that the virtual machine has spent waiting in the queue, ready to be scheduled on a CPU. An increase in this value indicates that the virtual machine is spending more time waiting and could be short on resources.
	<ul style="list-style-type: none"> • Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.
	<ul style="list-style-type: none"> • CPU. The current amount of CPU resources used by the virtual machine, expressed as a percentage.
	<ul style="list-style-type: none"> • Memory. The current amount of memory used by the virtual machine, expressed as a percentage.
	<ul style="list-style-type: none"> • Network. The current network transfer rate for the virtual machine.
	<ul style="list-style-type: none"> • Storage. The current disk transfer rate for the virtual machine.
	<ul style="list-style-type: none"> • Operating System. The name of the operating system.
	<ul style="list-style-type: none"> • IP Address. The primary IP address for the virtual machine.

Overview of Detail views

Detail views are drill down views accessible from some tile views.

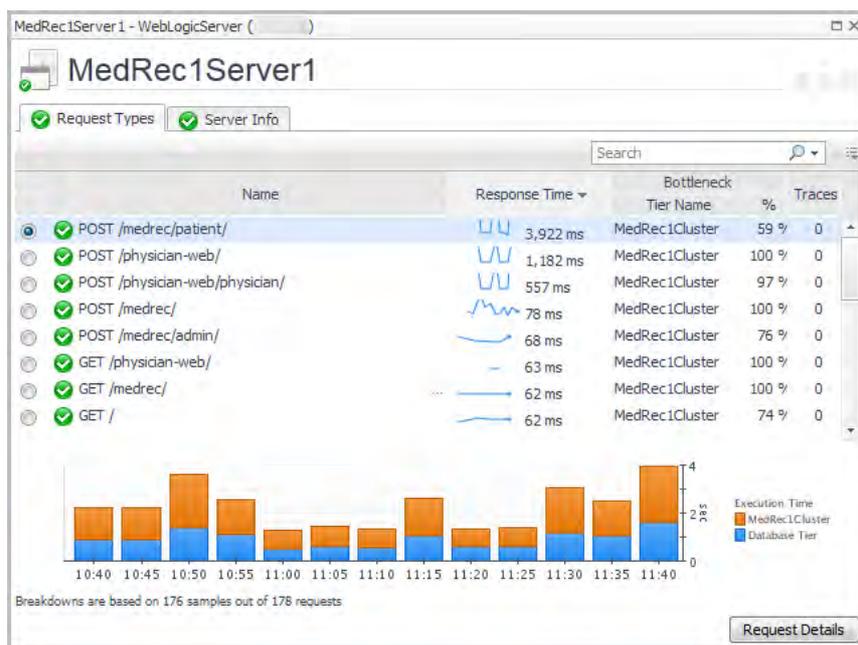
For more information about a specific view, see:

- [Application Server detail view](#)
- [Host detail view](#)
- [Pivot Breakdown detail view](#)
- [Real User \(APM\) Performance detail view](#)
- [Real User \(FxM\) Performance detail view](#)
- [Synthetic Result detail view](#)
- [Synthetic User Performance detail view](#)
- [Virtual Machine detail view](#)

Application Server detail view

The Application Server detail view provides a list of Request Types, as well as server information for the selected application server.

Figure 73. Example of an Application Server detail view



The **Request Types** tab lists the following information for each request type: request name, response time, bottleneck location (based on the most time-consuming tier of a request), calls completed, calls incomplete, call exceptions, and number of traces.

The chart shows the tier breakdown for the selected request.

The information presented on the **Server Info** tab depends on the type of application server selected: JBoss®, OracleAS, Apache Tomcat, WebSphere®, or WebLogic®.

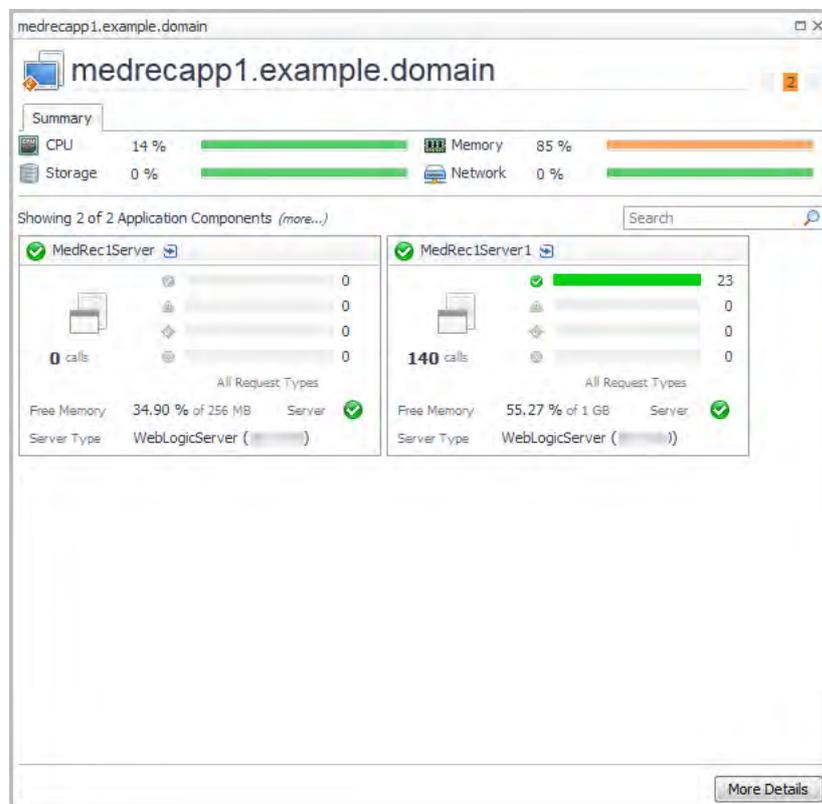
Next Steps:

- To drill down for detailed information about a selected request, click **Request Details**.

Host detail view

The Host detail view provides high-level host health, and tiles for any application components running on the selected host.

Figure 74. Example of a Host detail view



The banner shows host metrics if the host is monitored. Click **More Details** to see the performance details for the host.

If the host is not monitored, then:

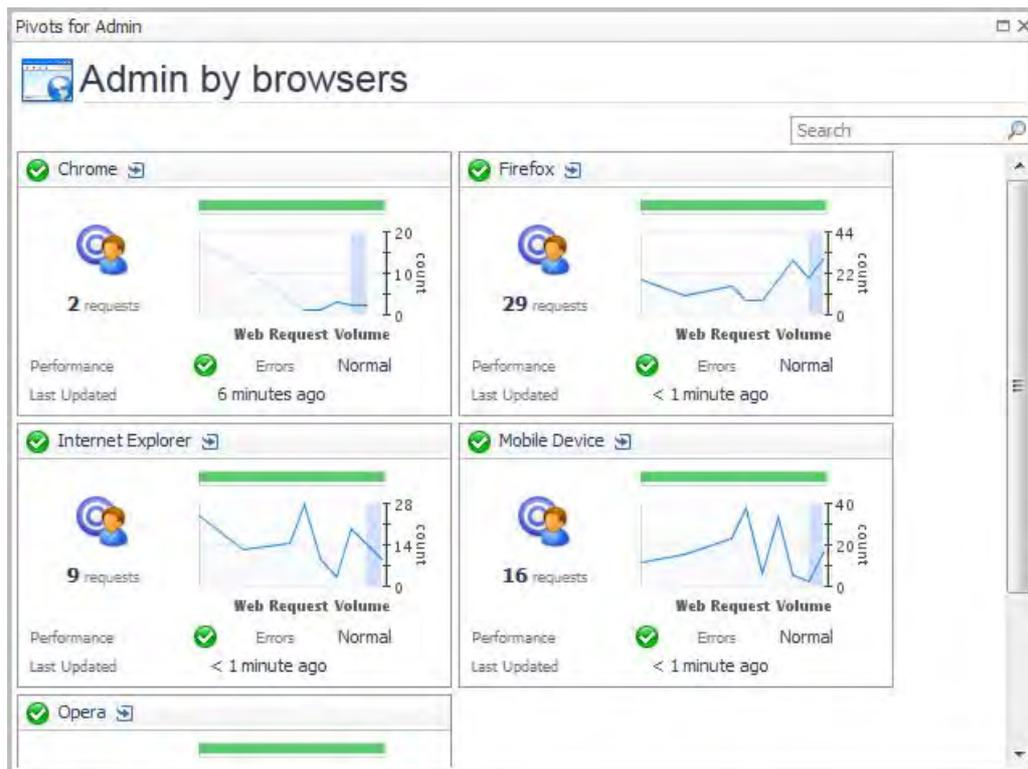
- If the host is not part of a Federated environment, and the Foglight Cartridge for Infrastructure is installed, click **Add OS Monitor** to configure host monitoring. For information, see the *Foglight for Infrastructure User and Reference Guide*.
- If the host is a Federation Master, the banner shows a message indicating that the host is not monitored.
- If the host is not part of a Federated environment, and the Cartridge for Infrastructure is not installed, the banner shows a message indicating that the Cartridge for Infrastructure is required for host monitoring.

Pivot Breakdown detail view

The Pivot Breakdown detail view provides a tile for each pivot type that is included in the pivot roll up tile you clicked. For example, for a web browser pivot roll up tile, the breakdown detail view can include tiles for each of the following browser types: Chrome™, Firefox®, Internet Explorer®, Mobile Devices, and Opera™.

Each tile displays: requests, request volume, overall health, performance and error status, and the last updated time. For more information, see [Pivot tiles](#).

Figure 75. Example of a Pivot Breakdown detail view



From here you can:

- Click the title bar of any single pivot tile in this view to open a [Hits and Pages tabs](#) view.

Real User (APM) Performance detail view

The Real User (APM) Performance detail view provides detailed metrics for a single location real user transaction, including average response times, response time breakdowns, application infrastructure, and more.

To access this view, click the title bar of a [Real User \(APM\) tile](#), or from the Geographical Perspectives dashboard, click Transaction Detail for an APM transaction.

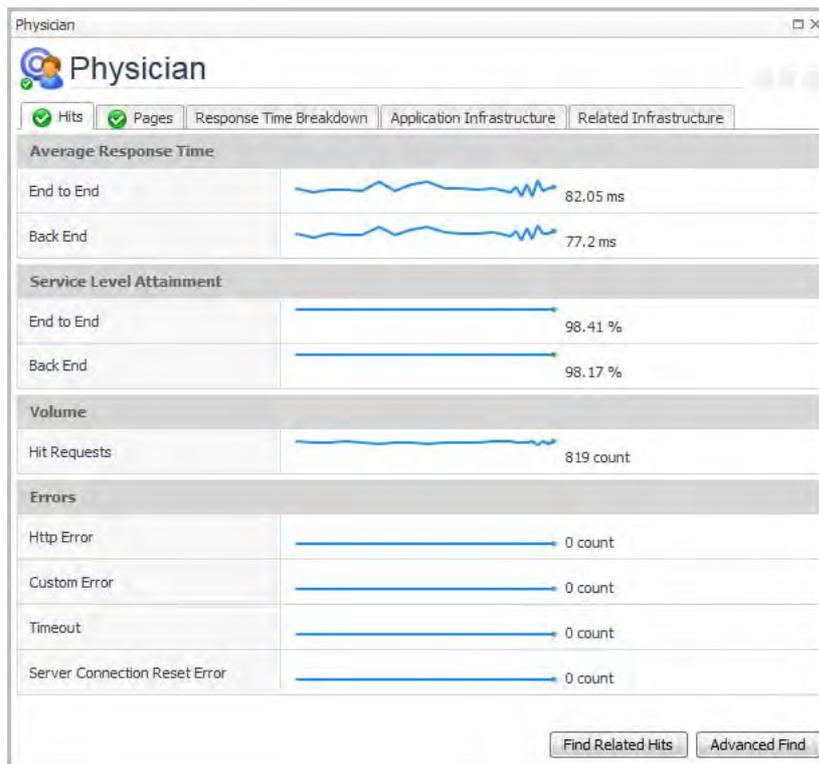
For more information, see the following topics:

- [Hits and Pages tabs](#)
- [Response Time Breakdown tab](#)
- [Application Infrastructure tab](#)
- [Related Infrastructure tab](#)

Hits and Pages tabs

The Hits tab and the Pages tab provide a summary of key metrics such as average response time, service level attainment, request volume, and errors.

Figure 76. Example of the Hits tab view



From here you can:

- Click **Find Related Hits** to open the Search Hits page.
- Click **Advanced Find** to open a list from which you can select a specific type of search. Choose from hits with: back end violations, end to end violations, or errors. The Hit Search runs with your selected criteria. Any results are returned on the Search Hits page.

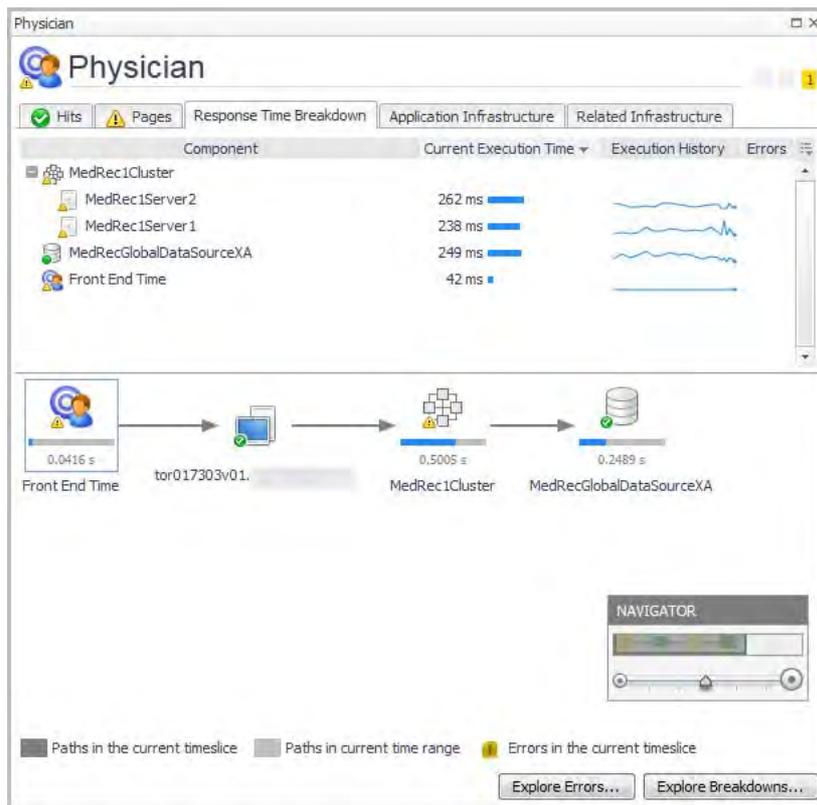
NOTE: If you have opened the Pages tab and you click Advanced Find, the drill down options are limited to captured pages.

Response Time Breakdown tab

The Response Time Breakdown tab displays a component-level breakdown of transaction execution times for the selected end user transaction group.

NOTE: The Response Time Breakdown Tab is visible only when Foglight for Java EE Technologies (version 5.8.2 or later), or Foglight for Microsoft .NET (version 5.9.1 or later) is installed and configured on your Management Server.

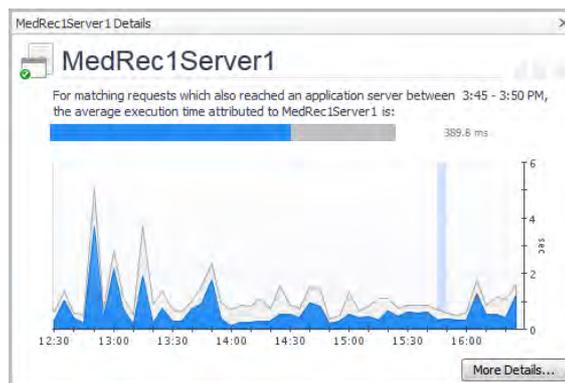
Figure 77. Example of the Response Time Breakdown tab view



From here you can:

- Click **Explore Errors** .
- Click **Explore Breakdowns** .
- Click a component icon to open the historical execution time chart.

Figure 78. Example of a historical execution time chart for a selected component



This chart provides a comparison of the average execution time for the selected component (in blue), overlaid on the total average execution time for the transaction (in grey). The vertical blue bar on the chart indicates the current timeslice.

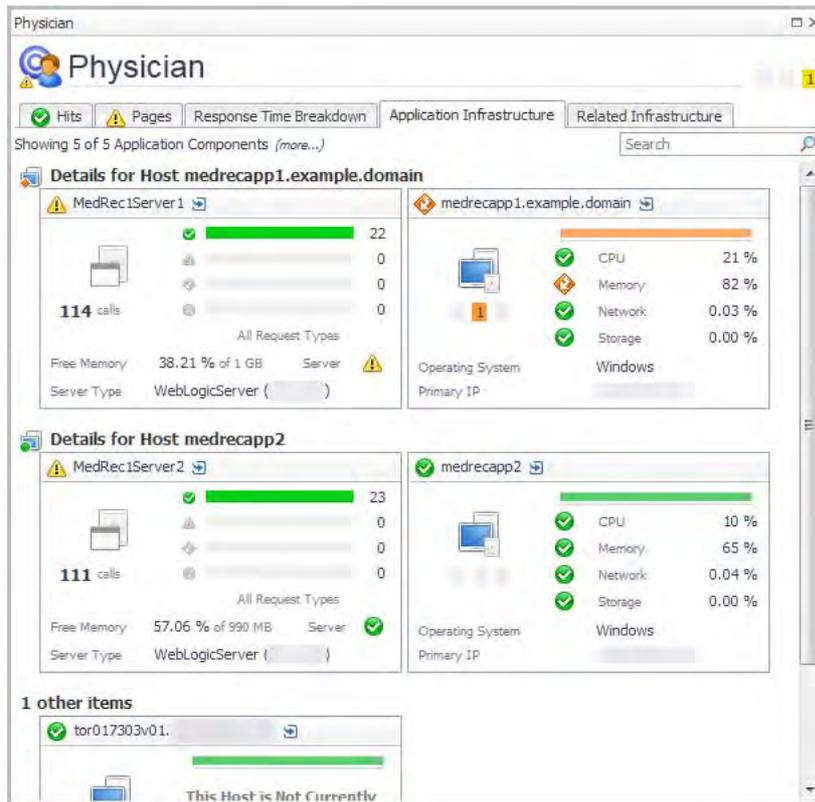
TIP: If you click a datasource component icon, the details view also includes a **Map to Application Component** button.

Click **More Details** to drill down to a detailed view of the selected application component. For example, from an application server component, you can access the Java™ application server details view.

Application Infrastructure tab

The Application Infrastructure tab includes a summary tile for each application component included in the transaction (for example, application servers, hosts, and databases).

Figure 79. Example of the Application Infrastructure tab view



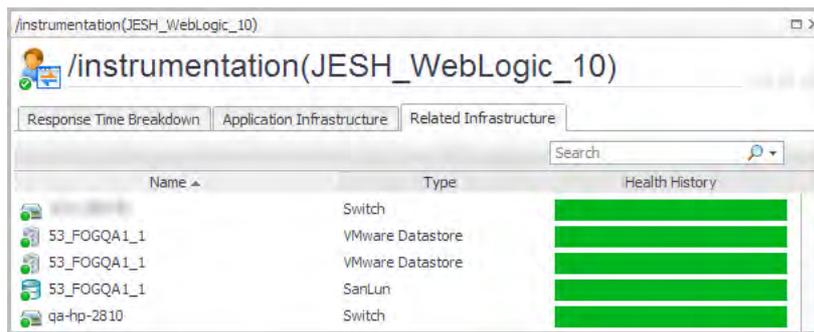
From here you can:

- Click the title bar of any application component tile to drill down to a detail view for that component type. For example, drilling down on a WebLogic® Server tile opens the [Application Server detail view](#).
- Add monitoring to an unmonitored host. If a host tile displays the message “This Host Is Not Currently Being Monitored,” click the title bar to open a [Host detail view](#), where you can add host monitoring.

Related Infrastructure tab

The Related Infrastructure tab displays a list of related infrastructure components, such as NMS devices, virtual machines (VMs) and ESX® servers, and devices managed by Foglight™ for Storage Management.

Figure 80. Example of the Related Infrastructure tab view



From here you can:

- Click on a device name to drill down to a view for that device type.

Table 46. Device icons and related drill-down views

Icon	Component Type	Drill-down view
	Switch or Router (Managed NMS devices)	A pop-up summary view that shows key metrics such as transfer rate, network and CPU utilization, memory usage, and packet rates.
	VMware® Datastore	VMware Explorer > Datastore Performance view.
	SanLun (Managed storage device)	Storage Manager topology view.

Real User (FxM) Performance detail view

The Real User (FxM) Performance detail view provides detailed metrics for a single location real user transaction, including time spent in front-end and back-end, SLA and OLA attainment, page request volume, and more.

To access this view, click the title bar of a [Real User \(FxM\) tile](#), or from the Geographical Perspectives dashboard, click Transaction Detail for an FxM transaction.

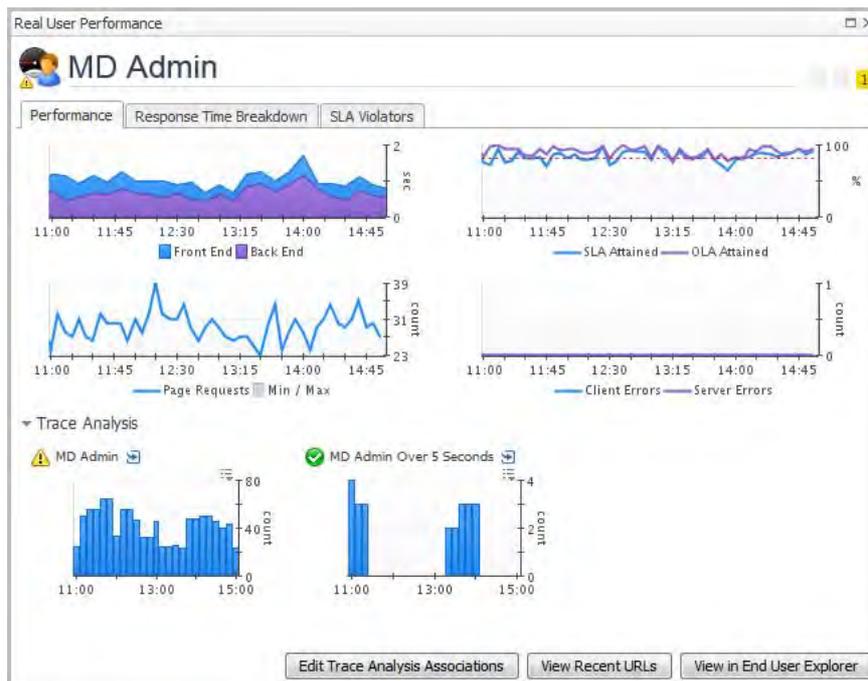
For more information, see the following topics:

- [Performance tab](#)
- [Response Time Breakdown tab](#)
- [SLA Violators tab](#)

Performance tab

The Performance tab displays charts of performance metrics and trace analysis information.

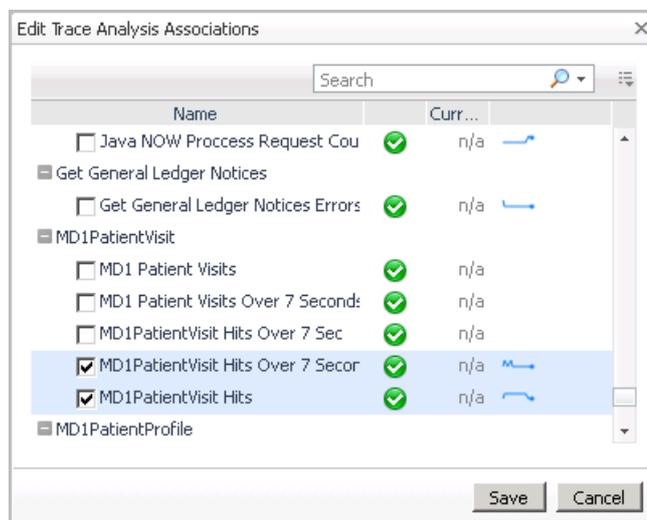
Figure 81. Example of the Performance tab view



From here, you can:

- Click a Trace Analysis chart to drill down to the data in Foglight Experience Viewer (FxV).
- Click **Edit Trace Analysis Associations** to view and edit the state of the available counters that represent statistics for the monitored application. Select one or more of the available counters in the **Edit Trace Analysis Associations** dialog box to display their statistics in the Real User Performance detail view, under Trace Analysis.

Figure 82. Edit Trace Analysis Associations dialog box



NOTE: This is only possible if your monitoring environment includes an FxV Appliance and the Cartridge for FxV is installed on the Management Server.

- Click **View Recent URLs** to drill down to the Foglight Experience Monitor (FxM) views and data.

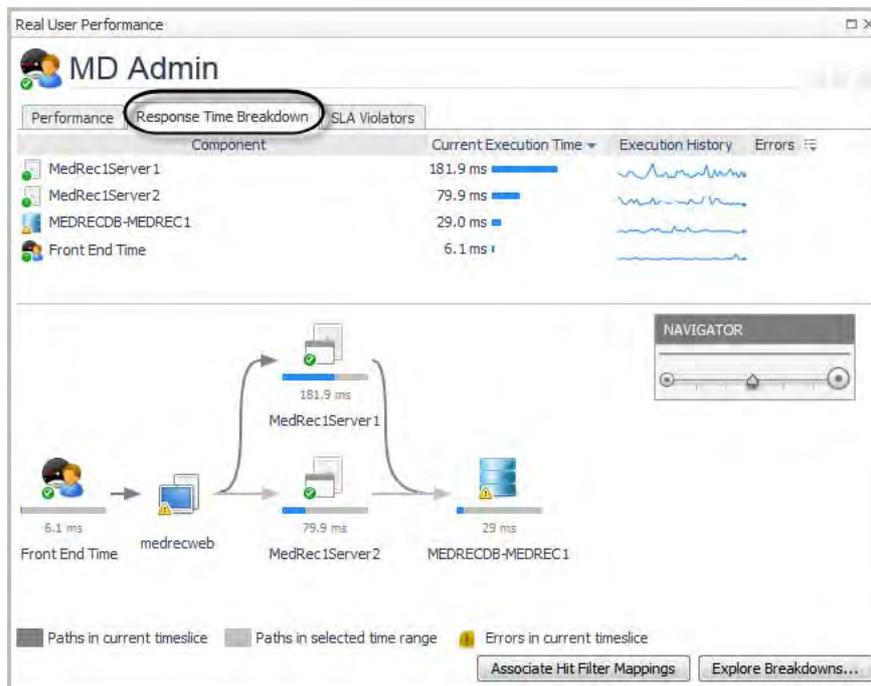
- Click **View in End User Explorer** to see the application statistics in the End User Explorer dashboard. For more information about this dashboard, see the *Managing the Cartridge for FxM User and Reference Guide*.

Response Time Breakdown tab

The Response Time Breakdown tab displays a component-level breakdown of transaction execution times for the selected end user transaction group.

- NOTE:** The Response Time Breakdown Tab is visible only when Foglight for Java EE Technologies (version 5.8.2 or later), or Foglight for Microsoft .NET (version 5.9.1 or later) is installed and configured on your Management Server.

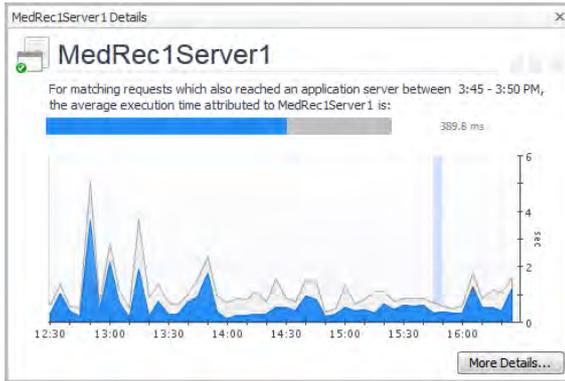
Figure 83. Example of the Response Time Breakdown tab view



From here you can:

- Click **Associate Hit Filter Mappings**.
- Click **Explore Breakdowns**.
- Click a component icon to open the historical execution time chart.

Figure 84. Example of a historical execution time chart for a selected component



This chart provides a comparison of the average execution time for the selected component (in blue), overlaid on the total average execution time for the transaction (in grey). The vertical blue bar on the chart indicates the current timeslice.

TIP: If you click a datasource component icon, the details view also includes a **Map to Application Component** button.

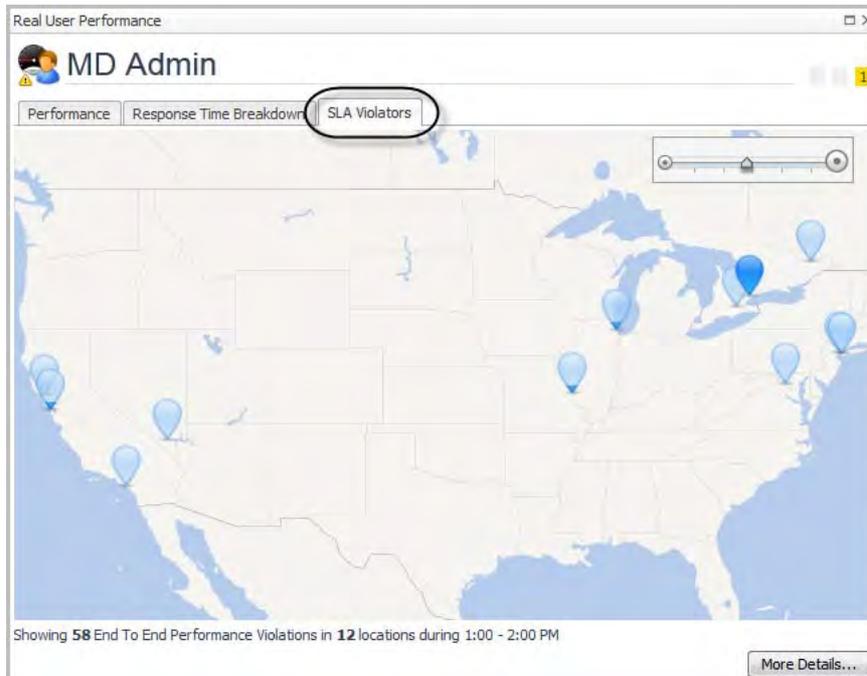
- Click **More Details** to drill down to a detailed view of the selected application component. For example, from an application server component, you can access the Java™ application server details view.

SLA Violators tab

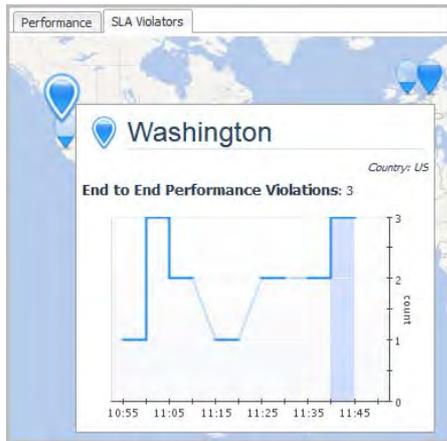
The SLA Violators tab provides a map view that helps you determine if your SLA violations are geographic in nature.

NOTE: This view is only available if the specific application has been configured for mapping.

Figure 85. Example of the SLA Violators tab view



Hover the cursor over a location indicator to view a graph of the service level performance for that location.



Click a location indicator to open the Location Detail view for that location. For more information, see [Viewing real user activity from a geographical perspective](#).

Click More Details on the SLA Violators tab to open the Geographical Perspective dashboard. For more information, see [Viewing real user activity from a geographical perspective](#).

Synthetic Result detail view

The Synthetic Result detail view provides detailed metrics for a single location synthetic transaction, including health, response time, and a summary of executions.

Figure 86. Example of the Synthetic Result detail view

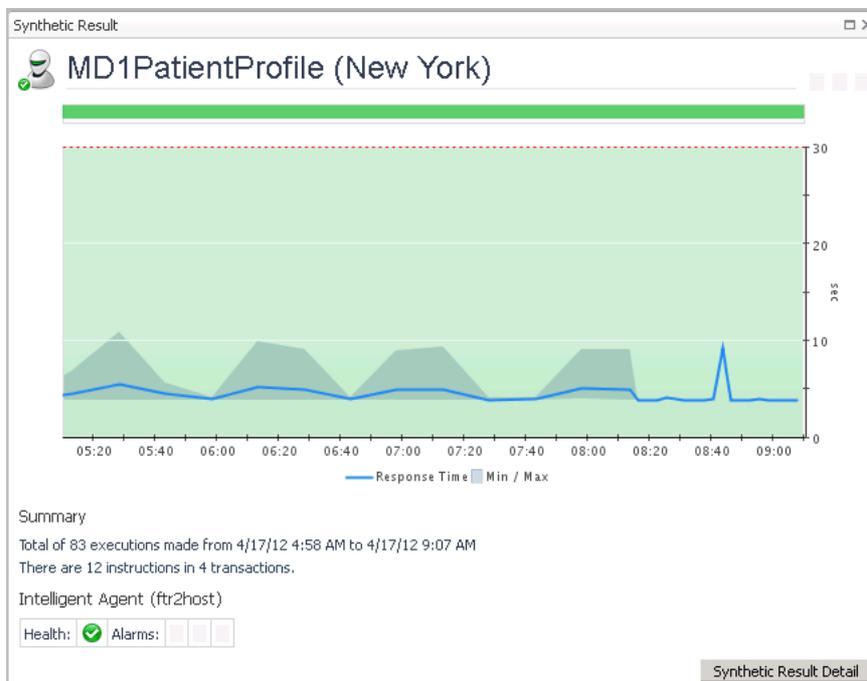


Table 47. Description of the Synthetic Results detail view

Data displayed	<p>Health History Bar. The color-coded bar represents the alarm state of the monitored component over the time range selected in the SOC. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.</p>
	<ul style="list-style-type: none"> • Response Time. A chart of the response time for the transaction. The shaded background
	<ul style="list-style-type: none"> • Summary. Provides the total number of executions over the given time range, and the number of instructions for transaction.
	<ul style="list-style-type: none"> • Health. This icon indicates the transactions overall health status.
	<ul style="list-style-type: none"> • Alarms. Indicates how many of each type of alarm (Fatal, Critical, Warning) occurred in the selected time range.

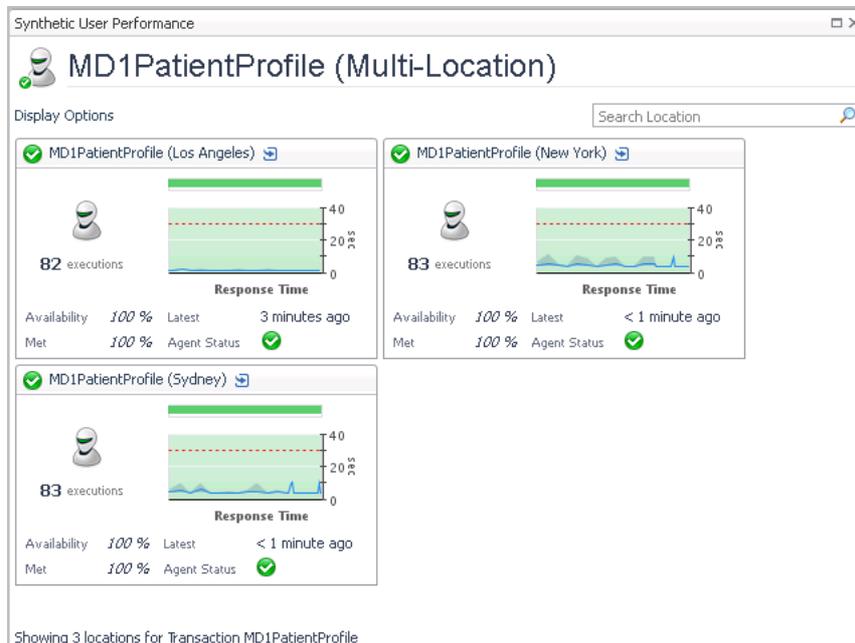
From here, you can:

- Click **Synthetic Result Detail** to see the script execution statistics in the End User Explorer dashboard. For more information about this dashboard, see the *Foglight Transaction Player User and Reference Guide*.

Synthetic User Performance detail view

The Synthetic User Performance detail view provides a container view of results from all locations for a selected synthetic transaction. Each location is displayed in a single tile view that provides the same information as the [Single-Location Synthetics](#) tile.

Figure 87. Example of the Synthetic User Performance detail view

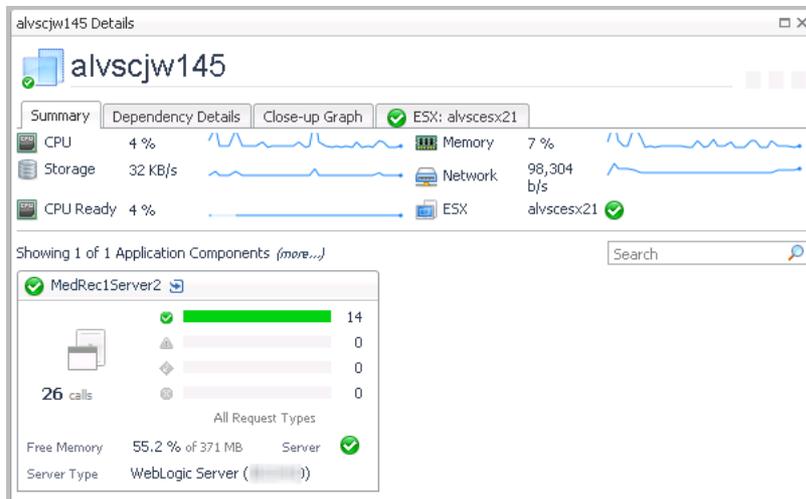


Click the title bar of any tile to drill down to the [Synthetic Result detail view](#) for that location.

Virtual Machine detail view

The Virtual Machine (VM) detail view provides high-level performance metrics for both the currently selected VM and for its host ESX[®] Server, and tiles for any application components running on the selected VM.

Figure 88. Example of the Virtual Machine detail view



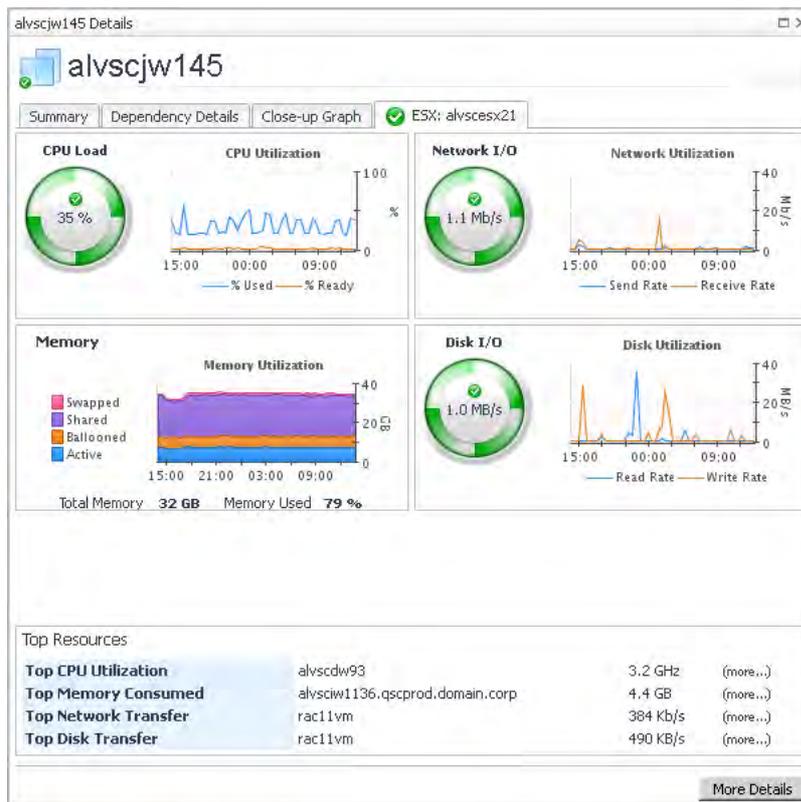
From here, you can:

- Click the ESX: *<hostname>* tab to access the [ESX Server detail view](#).
- Click **More Details** (not shown, located at the bottom right corner of the view) to drill down to a vmExplorer view.
- Click the title bar of an application component tile to open the detail view for that component.

ESX Server detail view

This tab displays the CPU, Memory, Network, and Disk utilization for the *<hostname>* from the perspective of the ESX[®] server. The lower part of the tab displays the top resource consumers for this host. From this tab you can navigate to the vmExplorer dashboard by clicking **More Details**. This dashboard allows you to further investigate the performance of the selected ESX[®] host.

Figure 89. Example of the ESX Server detail view



From here, you can:

- Click **More Details** to drill down to a vmExplorer view.

Topology object name reference table

The following table provides the domain and topology object names you need to use to ensure the tiles appear correctly for a manually built service.

Table 48. Topology object name reference

Domain	Topology Object
.NET	.NETApplicationInstance
Apache	ApacheSvrAgent
AppMonitor	AppMonitorAgent
APM Appliance (hits)	EUHitInteraction
APM Appliance (sequences)	EUSequenceInteraction
Custom Application Transactions (Java™ EE and .NET®)	CustomApplicationTransaction
DB2	DB2_Instance
FTR	FTRResult
FxM	FxMApplicationResult
Host ¹	Host
Java EE Technologies	JavaEEAppServer
JMX	JMXServer

Table 48. Topology object name reference

Domain	Topology Object
Log Filter	LogFilterAgent
MQ Series	MQQueueManager
Oracle	DBO_Instance
SQL Server	DBSS_Instance
Sybase	Sybase_MDAAgent
WebMonitor	WebMonitorAgent

1. For hosts, always select the host object, regardless of whether or not the host is virtual (for example, Hyper-V® or VMware®). Foglight looks for the appropriate host extensions and displays the associated host dashboard (physical or virtual).

NOTE: The list of available topology objects is current as of this release. Additional cartridges may add additional relevant objects in future releases.

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.software.dell.com.

Contacting Dell

Technical support:

[Online support](#)

Product questions and sales:

(800) 306-9329

Email:

info@software.dell.com

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to <https://support.software.dell.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. In addition, the portal provides direct access to product support engineers through an online Service Request system.

The site enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to [Trial Downloads](#).
- View how-to videos
- Engage in community discussions
- Chat with a support engineer