

Foglight® for Active Directory 6.3.0
User and Reference Guide



© 2023 Quest Software Inc.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

owners.

Legend

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

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

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

Foglight for Active Directory User and Reference Guide
Updated - 2023
Foglight Version - 6.3.0
Cartridge Version - 6.3.0

Contents

Navigation basics	8
Foglight browser interface panels	8
Navigation panel	9
Display panel	9
Action panel	9
Drill down actions	10
Breadcrumb trail	10
Time range	10
Lists	11
Sorting content	11
Hiding columns	11
Filtering content	12
Alarms and state indicators	13
Mouse-over actions	13
Foglight for Active Directory roles	14
Exploring Foglight for Active Directory dashboards	15
Accessing the Foglight for Active Directory dashboards	15
Active Directory Alarms dashboard	16
Active Directory Environment dashboard	17
Active Directory Environment > Monitoring tab	18
Active Directory Environment > CA Health Check tab	21
Active Directory Environment > Administration tab	22
Active Directory Environment > Reports tab	22
Active Directory Environment > FAQs tab	25
Active Directory Explorer dashboard	27
Active Directory Enterprise view	27
Active Directory Explorer Primary view	29
Active Directory Rule Management dashboard	32
Managing Active Directory agents	33
Agent Status dashboard	33
Active Directory/Certificate Authority agent management	33
Tasks list	34
Agent Management view	34
Managing certificates	42
Active Directory agent properties	46
Configuration	47
Monitor	49
Unavailable WMI Classes	49
Data Collection Scheduler	49
Reporting on your Active Directory enterprise	51
Foglight for Active Directory reports	51

Foglight for Active Directory views	54
Forest views	54
Forests Environment Summary (All Forests) view	54
Forest Environment Summary view	55
Forests Explorer Summary (All Forests) view	56
Forest Explorer Summary view	57
Domain views	59
Domains Environment Summary (All Domains) view	59
Domain Environment Summary view	60
Domains Explorer Summary (All Domains) view	61
Domain Explorer Summary view	62
Site views	63
Sites Environment Summary (All Sites) view	63
Site Environment Summary view	64
Sites Explorer Summary (All Sites) view	65
Site Explorer Summary view	66
Domain Controller views	67
Domain Controllers Environment Summary (All DCs) view	67
Domain Controller Environment Summary view	68
Domain Controllers Explorer Summary (All DCs) view	69
Domain Controller Explorer Summary view	70
Resource Utilization Details view	71
Domain Controller Database view	72
Domain Controller Directory Services view	74
Domain Controller DFS-R view	75
Domain Controller FRS view	76
Domain Controller Replication view	77
Description of embedded views	78
Address Book view	80
Agent State view	81
Asynchronous Thread Queue view	81
Core Services view	81
Database Access view	82
Database Cache view	83
Database Log Access view	83
Database Performance Health view	84
Defragmentation Tasks view	85
DFS Namespace Service API Queue view	85
DFS Namespace Service API Requests view	86
DFS Namespace Service Referrals view	86
DFS Replicated Folders view	87
DFS Replication Connections view	88
DFS Replication Service Volumes view	89
DFS-R Performance Health view	90
Directory Replication Inbound view	91
Directory Replication Outbound view	92
Directory Replication Sync view	92
Directory Replication USN view	93

Directory Services General view	94
Directory Services Performance Health view	95
Directory Services Reads view	96
Directory Services Searches view	96
Directory Services Writes view	97
Domain Controller Details view	97
Domain Controllers view	98
FileReplicaConn Authentications/Bindings view	99
FileReplicaConn Change Orders view	99
FileReplicaConn Fetch view	100
FileReplicaSet Authentications/Bindings view	101
FileReplicaSet Change Orders view	101
FileReplicaSet DS Communications view	102
FileReplicaSet Files view	103
FileReplicaSet Local Change Orders view	103
FileReplicaSet Packets view	104
FileReplicaSet Remote Change Orders view	105
FRS Performance Health view	106
FRS Replica Sets view	107
FRS Staging Files view	107
FSMO Roles view (Domain)	108
FSMO Roles view (Forest)	109
Host Monitor view	109
Inter-Site Transports view	109
Inventory By Category view	110
IP Subnets view	111
Key Distribution Center view	111
LDAP view	111
Memory view	112
Network view	113
Processor view	113
Replication Performance Health view	114
Resource Utilization view	115
Security Accounts Manager view	116
Server Health view	117
Statistics view	118
Storage view	118
Summary and Resource Information view	119
Top AD Metrics view	119
Top 3 Consumers view	122
Top 3 CPU Consumers view	123
Top 3 DS Directory Reads/sec view	123
Top 3 LDAP Bind Times view	123
Top 3 Memory Consumers view	123
Top 3 Network Consumers view	124
Top 3 Replication Queue Length view	124
Top 3 Storage Consumers view	124
Trusts view	125

USN Records view	125
Foglight for Active Directory rules	127
Rules dashboard	127
Active Directory Rule Management dashboard	128
Managing Foglight for Active Directory rules	130
Rules reference	131
Running diagnostic tests	132
Diagnostic Tests dashboard	132
Tasks list	132
About Diagnostic Test Types pane	135
Diagnostic Tests list	135
Diagnostic Tests reference	137
DNS Entries diagnostic	137
DNS Partners diagnostic	138
File Replication diagnostic	138
FSMO Best Practices diagnostic	139
GPO Sync diagnostic	139
Hotfix and Service Pack diagnostic	140
Replication Failure diagnostic	140
Replication Link diagnostic	140
Schema Consistency diagnostic	141
Service Status diagnostic	141
Site Configuration diagnostic	141
Time Differential diagnostic	142
Time Parent Sync diagnostic	142
Track Replication diagnostic	143
Managing Active Directory metrics	144
Agent Status and Agent Properties dashboards	144
Active Directory Metrics Management dashboard	145
Managing Active Directory metrics	147
Using the Metrics Management dashboard	147
Using the Agent Status and Agent Properties dashboards	149
About Us	150
We are more than just a name	150
Our brand, our vision. Together.	150
Contacting Quest	150
Technical support resources	150

Navigation basics

This guide has been prepared to assist you in becoming familiar with Foglight for Active Directory. It provides basic navigation techniques, describes the dashboards, views, and reports included with the Foglight for Active Directory, and provides information about the rules that are available for your monitored system.

This section describes the basic techniques used to navigate through Foglight for Active Directory. It is intended to introduce you to the layout of the Foglight user interface and how to navigate through the dashboards and views provided with Foglight for Active Directory.

- [Foglight browser interface panels](#)
- [Drill down actions](#)
- [Breadcrumb trail](#)
- [Time range](#)
- [Lists](#)
- [Alarms and state indicators](#)
- [Mouse-over actions](#)
- [Foglight for Active Directory roles](#)

For more information about Foglight navigation, see the *Foglight User Guide* or online help.

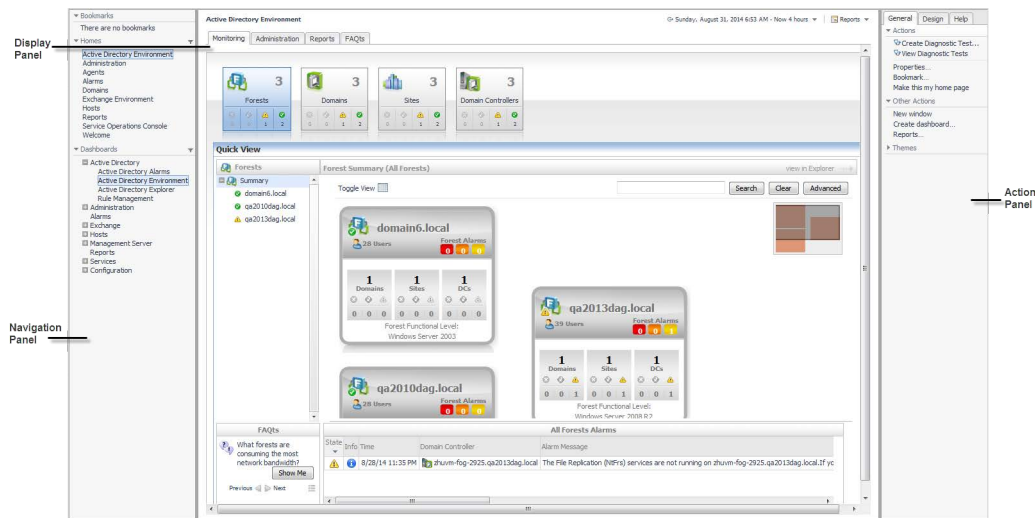
Foglight browser interface panels

Depending on who you log in as, you may see either the contents of the first bookmark (the Welcome page is the default) listed under Bookmarks, or a home page. For further details about these Foglight pages, see the *Foglight User Guide* or online help.

Typically the browser interface is divided into three panels:

- [Navigation panel](#)
- [Display panel](#)
- [Action panel](#)

Figure 1. Foglight browser interface



Navigation panel

The navigation panel, at the left of the browser interface, operates like a drawer and is open by default. To close the navigation panel, click the arrow to the far left of the Foglight browser interface. Click the arrow again to open the navigation panel.

The navigation panel contains an expandable view of all the dashboards available to the current user. To access a specific dashboard, open the appropriate module (for example, Active Directory) and select the dashboard to view it in the display panel.

The navigation panel also provides access to the Foglight Administration and Configuration areas, and may provide access to some cartridge-specific navigational views (for example, the Active Directory Enterprise view for the Active Directory Explorer dashboard.)

If you do not see any dashboards in the navigation panel, the user ID with which you signed in may not have been assigned to a group. For details, see the *Foglight User Guide* or online help.

Display panel

The display panel is the large panel in the middle of the browser interface and is used to view current dashboards and reports, as well as to create new dashboards and reports. You can increase the size of the display panel by resizing the navigation panel, or if open, by closing the action panel.

Action panel

The action panel, at the right of the browser interface, operates like a drawer and is closed by default. To open the action panel, click the arrow to the far right of the Foglight browser interface. Click the arrow again to close the action panel.

The action panel lists the actions and tasks you can perform within the currently displayed dashboard. It also contains the views and data that you can add to a dashboard or report, and provides access to the online help files.

Drill down actions

Use the graphical and text links in views to drill down to additional details that may assist you in diagnosing problems. Depending on the link, you drill down to a different dashboard or smaller view called a popup that appears over the dashboard you are currently viewing.

You can drill down from many different parts of a view, including names of monitored components (such as forests and domain controllers), the **view in Explorer** links in a dashboard, and items like charts, tables, cylinders and icons.

NOTE: When your cursor is positioned over a drillable component, the cursor will change to a selector icon, typically a hand with a pointing finger.

For example, in the Forest Environment Summary (Individual Forest) view in the Active Directory Environment dashboard, click the DNS Servers heading in the Inventory By Category view. A Domain Controller Inventory popup appears that lists the domain controllers (DCs) that are designated as DNS servers. Click a DC in this list to drill down further to explore the selected DC's health and alarms to diagnose problems.

Breadcrumb trail

As you drill down into more detailed views within a dashboard, the names of the previous views are displayed in a breadcrumb trail at the top of the current dashboard. In addition to providing you with context, this breadcrumb trail displays the name of the current view and provides a simple mechanism for returning to any of its parent levels.

The following breadcrumb trail was created while drilling down from the Active Directory Environment dashboard into the Rule Management dashboard. Each item within the breadcrumb trail is a link to a previously viewed parent level.

Figure 2. Breadcrumb trail



Time range

By default, Foglight for Active Directory displays metrics, alerts and messages that have occurred within the last four hours. This time range is configurable using the Time Range popup located in the upper right corner of the browser interface.

Figure 3. Time range



Using the Time Range popup, you can select from predefined time ranges or you can specify a custom range using either the slide time bar or calendar precision controls to specify a date and time. When you modify the time range for a dashboard or view, it adjusts the range for all of the views contained within and drilldowns accessed from that dashboard or view. It does not adjust the time range for any parent views.

For more information about modifying the time range, see the *Foglight User Help*.

Lists

The lists displayed throughout Foglight for Active Directory allow you to define the sort criteria and order, hide columns, and filter content based on user-defined search criteria:

- [Sorting content](#)
- [Hiding columns](#)
- [Filtering content](#)

Sorting content

Some views in Foglight for Active Directory dashboards contain sortable lists. An example of a sortable list is the Domain Controllers view on the Active Directory Explorer dashboard.

Figure 4. Domain Controllers view

State	Name	IP Address	Purpose	Roles	CPU	Memory	Bytes In	Bytes Out	Replication	Operating System
	bdc.o3.local	10.6.177.12	Domain Controller	n/a	3.5 %	71.8 %	3.2 K/s	3.2 K/s		Win 2003 Server
	pdc.o3.local	10.6.177.11	Global Catalog	Multiple FSMO	5.8 %	84.0 %	3.2 K/s	3.2 K/s		Win 2003 Server

An arrow in the column heading identifies the sort criteria and order, ascending or descending, being used to display information.

To change the sort criteria in a list:

- 1 Click on the column heading to be used to sort the list.
- 2 The sort order is in ascending order, but can be changed to descending order by clicking on the heading a second time.

The list is redrawn according to your specification.

Hiding columns

Foglight for Active Directory lists display a default set of columns; however, you can customize the content of the lists by hiding columns.

To hide columns in the list:

- 1 Select the button in the upper right corner of the list to display the Show Columns dialog.
- 2 On the Show Columns dialog, click a column heading from the list to clear the corresponding check box.
- 3 Select **Apply** to display the list displaying only the columns that are currently selected in the Show Columns dialog.

Filtering content

Many of the lists displayed in Foglight for Active Directory dashboards and views allow you to filter the information displayed using the search controls at the top of the list. You can either conduct a search on all of the columns in the list or specify the columns to be searched.

Figure 5. Filtering content




To filter a list based on content in any of the fields:

- 1 Enter a text string into the text field.

NOTE: Select the Use Regular Expression option that appears when you select the arrow control to the right of the Search field to specify a regular expression which allows you to enter a search pattern using wildcard characters instead of a literal text string.

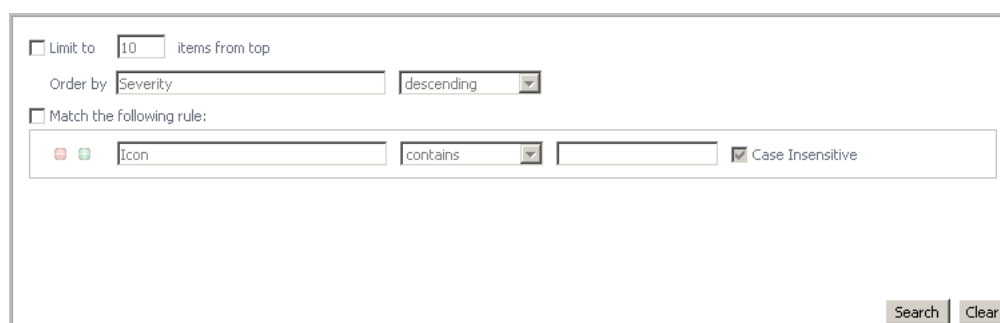
The list now displays the entries found as a result of your search.

- 2 To clear the search string and display the original list, select .

To specify individual fields to be searched:

- 1 Click the arrow control and select **Advanced Search**.



A dialog appears allowing you to enter the search criteria to be used to filter your list and sort the results.



The dialog box contains the following controls:

- ☐ Limit to: items from top
- Order by:
- ☐ Match the following rule:
 -
 - ☒ Case Insensitive
-





- 2 To define the number of items to be included in the list and the sort criteria and order of the results, select the **Limit to nn items from top** check box.
- 3 By default, the top 10 items are displayed. To change this value, enter a different number in the value field.
- 4 The **Order by** field contains the column heading currently selected as the sort criteria. To change the sort criteria, click in the **Order by** field and select the column heading to be used. Use the arrow control to define the sort order: ascending or descending.
- 5 To define the search criteria, select the **Match the following rule** check box and specify the following information:
 - Click in the first field to specify the column to be searched.
 - Use the arrow control to define the comparison operator to be used (for example, does not contain, starts with, ends with.)
 - Enter the text string to be matched.
 - The **Case Insensitive** check box is selected by default and will find matches regardless of case. For a case-sensitive search, clear this check box.

- 6 To add an additional search rule, select  and repeat the previous step to specify the additional search criteria.
- i | NOTE:** When multiple rules are specified, the 'and' operator is used and all rules must be met in order for an entry to be included in the search results.
- 7 Once you have entered your search criteria, select **Search** to close the dialog and conduct the search.
- 8 The results of your search is displayed in the list.
- 9 To clear the search string and display the original list, select .

Alarms and state indicators

Foglight for Active Directory uses state indicators to show the severity level of alarms that have fired or the status of an Active Directory® object. The following state indicators and colors are used throughout the product:

Table 1. Alarms and state indicators

	Fatal (red)	There is a strong indication that the server is experiencing conditions which will degrade performance.
	Critical (orange)	Indicates that the current metric values point strongly towards performance-related problems with the specified component.
	Warning (yellow)	Represents a possible performance problem, based on calculations on current server metrics against best-practices thresholds.
	Normal (green)	Indicates the component is operating within normal thresholds. A normal severity level indicates that there have been no warning, critical or fatal events fired. Foglight does not record events that are successful; it can only determine that there are no events that had problems.

The Foglight alarm types respond to thresholds that are defined within Foglight for Active Directory rules. As metrics change and move through thresholds, alarms are raised. As a metric moves through thresholds, the severity of an alarm changes, which causes the associated state indicators to change.

For detailed information about Foglight for Active Directory rules and metrics, see [Foglight for Active Directory rules](#).

Mouse-over actions

Many items within Foglight for Active Directory dashboards display additional information when you hover your cursor over them. For example:

- Hover over a graph title to display a description of the graph
- i | NOTE:** Clicking on a counter or graph displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.
- Hover over a data point in a graph to display details (actual value and date/time stamp) that corresponds to the data point

Foglight for Active Directory roles

Foglight controls user access using the concept of users, groups and roles. Each user can belong to one or more groups. The roles assigned to those groups determine the set of actions that the user can access.

Foglight comes with a set of built-in roles. In addition to these built-in roles, Foglight for Active Directory comes with the following additional built-in roles which control access to the dashboards in Foglight for Active Directory.

- **AD Administrator.** Allows access to all dashboards in Foglight for Active Directory.
- **AD QuickView User.** Allows access to the Active Directory Environment dashboard.
- **AD Report User.** When implemented, this role will allow access to the Report Management dashboard and Active Directory® reports.

i | NOTE: The AD Report User role is available starting with cartridges installed with Foglight Management Server 5.6.2.

The Users & Security dashboard allows you to manage user access. To access this dashboard, on the navigation panel, select **Dashboards > Administration > Users & Security Management**. For more information on managing users and security, see the *Foglight Administration and Configuration Guide* or online help.

Exploring Foglight for Active Directory dashboards

Foglight for Active Directory includes dashboards which aid in the monitoring, analysis and investigation of Active Directory® health and performance.

These dashboards provide real-time views into the present state and relationships of the major components in your Active Directory environment, including:

- **Forests** - the top-level object within the Active Directory infrastructure which consists of a group of Active Directory domains.
- **Domains** - a partition of the Active Directory forest used to implement directory security and manage resources.
- **Sites** - a logical grouping of computers within Active Directory that have reliable connectivity.
- **Domain Controllers (DCs)** - a server that is running a Windows Server® operating system and has Active Directory (or Active Directory Domain Services) installed, which is tasked with managing a replica of an Active Directory domain.

This section explains how to access the Active Directory dashboards, describes the layout of each dashboard, and explains how to navigate through the embedded views of each dashboard.

- [Accessing the Foglight for Active Directory dashboards](#)
- [Active Directory Alarms dashboard](#)
- [Active Directory Environment dashboard](#)
- [Active Directory Explorer dashboard](#)
- [Active Directory Rule Management dashboard](#)

For a description of the metrics captured in each of the embedded views, see [Foglight for Active Directory views](#).

Accessing the Foglight for Active Directory dashboards

To access the dashboards:

- 1 On the navigation panel, under Dashboards, click the expansion state box to the left of **Active Directory**.
- 2 Click one of the dashboard items.
 - Click **Active Directory Alarms** to display a list of the current alarms triggered within Foglight for Active Directory.
 - Click **Active Directory Environment** to display the Active Directory Environment dashboard, which includes the following tabs:
 - **Monitoring**: displays a summary of the Active Directory® objects being monitored and their current state.

- **CA Health Check:** displays a summary of the Certificate Authority servers being monitored.
- **Administration:** allows you to perform administrative tasks, including:
 - View and manage rules that exist in your environment.
 - View a list of diagnostic tests that are available, as well as run a test immediately or define a schedule for when a test is to be run.
 - View, edit and enable/ disable the optional metric collections that are configurable for Active Directory agents.
 - Download and run a script for configuring Certificate Authority agent settings
 - Deploy the Active Directory agent package, create and activate Active Directory agents, and start or stop collecting data.
 - Deploy the Certificate Authority agent package, create and activate Certificate Authority agents, and start or stop collecting data.
- **Reports:** allows you to build, view, and manage custom reports.
- **FAQTs:** displays questions relating to a selected object.
- Click **Active Directory Explorer** to display performance metrics and alarms for an Active Directory object type container or individual object.
- Click **Rule Management** to view and manage Foglight for Active Directory rules.

Active Directory Alarms dashboard

The Active Directory Alarms dashboard shows the alarms that have been triggered but not cleared within Foglight for Active Directory. It can be used to isolate alarms specific to your Active Directory® environment.

Figure 6. Active Directory Alarms dashboard






Active Directory Alarms Saturday, March 19, 2016 12:01 AM - Now 4 hours Reports

Alarms

Severity	Server	Time	Cleared	Cleared By	Instance	Alarm Message
Warning	zhuvn-fog-3336-afog.local	3/19/16 2:17 AM	Yes	system	zhuvn-fog-3336-afog.local	DNS Total Queries Received/sec are trending upward on this DC. This could result in issues with DNS-dependent services.
Warning	zhuvn-fog-3336-afog.local	3/18/16 7:19 PM	No		zhuvn-fog-3336-afog.local	DS Directory Reads/sec are trending upward on this DC - this could result in issues with LDAP-dependent services and machines.
Warning	zhuvn-fog-3336-afog.local	3/18/16 7:11 PM	No		zhuvn-fog-3336-afog.local	The File Replication (NFRs) services are not running on zhuvn-fog-3336-afog.local. If your domain is using FRS, this may cause client issues. Please keep this service running. If your domain is using DFSR, to keep clear of this alarm, navigate to Active Directory -> Rule Management, find & click AD Host DFSR Services rule, in the Warning severity, uncheck the "Active" box.
Error	DC2012R2-FogQA.local	3/18/16 6:11 PM	No		AD0-DC2012R2-FogQA.local	The Active Directory agent AD0-DC2012R2-FogQA.local started data collection failed. Error message: "com.quest.glue.api.services.NoCredentialsException: Could not establish a connection to host : DC2012R2-FogQA.local". Please download the agent log from Active Directory Environment->Administration->Agents to get more details.

The Alarms List displayed in the Active Directory Alarms dashboard is a sortable list that displays the outstanding Foglight for Active Directory alarms. Each alarm row in the Alarms List contains the following information.

Table 2. Alarms List information

Object	The icon in the first column identifies the source of the alarm:
	 Domain Controller
	 Domain
	 Forest
	 Site
	 General Active Directory® (not DC, Domain, Forest or Site)
Severity	The icon in this column indicates the severity of the alarm.
Server	Displays the name of the DC where the alarm occurred. Clicking the DC name displays a popup menu where you can choose to view details about the selected DC in either the Active Directory Explorer dashboard or Quick View.
Time	Displays the date and time when the alarm occurred.
Cleared	Displays whether the alarm was cleared.
Cleared By	For cleared alarms, displays the users who cleared the alarm.
Instance	Displays the name of the DC instance where the alarm occurred. Clicking the instance name displays a popup menu that provides health and alarm information for the selected instance.
Alarm Message	Displays the alarm message.

Clicking an alarm's severity icon, object icon, alarm message or time displays a popup where you can acknowledge or clear the alarm. This popup provides pertinent information about the selected alarm, such as the rule of origin of the alarm, the history of the alarm, and all of the notes attached to the alarm. For more information about managing alarms, see the *Foglight User Guide* or online help.

Active Directory Environment dashboard

The Active Directory Environment dashboard includes the following tabs:

- **Monitoring:** displays a summary of the Active Directory® objects being monitored and their current state. For details, see [Active Directory Environment > Monitoring tab](#).
- **CA Health Check:** displays a summary of the Certificate Authority objects being monitored.
- **Administration:** allows you to perform administrative tasks, including:
 - Create and activate Active Directory agents, and start or stop collecting data.
 - Create and activate Certificate Authority agents, and start or stop collecting data.
 - View and manage rules that exist in your environment.
 - View a list of diagnostic tests that are available, as well as run a test immediately or define a schedule for when a test is to be run.
 - View, edit and enable/ disable the optional metric collections that are configurable for Active Directory agents.
 - Download and run a script for configuring Certificate Authority agent settings.

NOTE: In a federated environment, the administrative tasks and Agents view are available only on the Federated Children and not on the Foglight Federation Master.

For details, see [Active Directory Environment > Administration tab](#).

- **Reports:** allows you to manage custom Active Directory reports. For details, see [Active Directory Environment > Reports tab](#).
- **FAQts:** displays questions relating to a selected object. For details, see [Active Directory Environment > FAQts tab](#).

Active Directory Environment > Monitoring tab

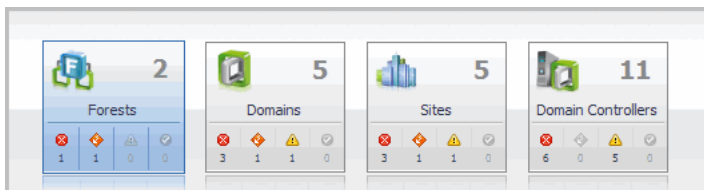
The Monitoring tab provides a summary of the Active Directory® components and consists of the following views:

- [Active Directory Environment Overview](#)
- [Quick View](#)

Active Directory Environment Overview

The Active Directory Environment Overview is located across the top of the Active Directory Environment dashboard. It provides you with an overview of your Active Directory® environment.

Figure 7. Active Directory Environment Overview view



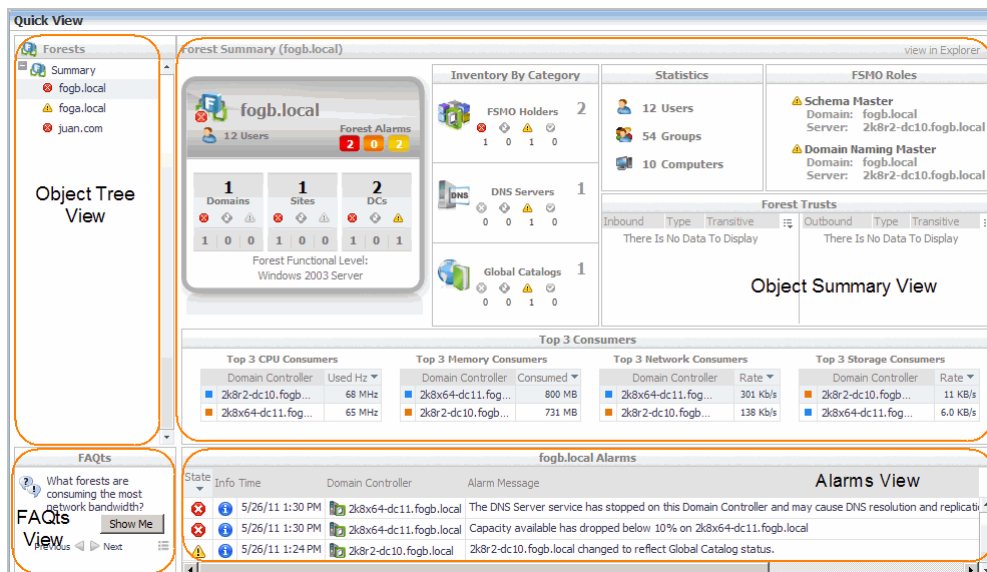
The overview contains a tile for the following object types in your Active Directory infrastructure: forests, domains, sites, and domain controllers. Each tile shows the number of corresponding objects of that type in your Active Directory infrastructure as well as a count of objects of that type in each of the alarm states (fatal, critical, warning, and normal).

Clicking a tile displays summary information for that object type in the Quick View. Clicking an alarm state (for example, warning) on a tile displays summary information in the Quick View for the objects of that type that are in the selected alarm state.

Quick View

The Quick View is located across the middle of the Active Directory Environment dashboard.

Figure 8. Quick View



Purpose

The Quick View displays summary information pertaining to the component selected from the Active Directory Environment Overview and Object Tree view. For example,

- Select an object tile in the Active Directory Environment Overview to view summary information for all objects of the selected type.
- Select an alarm indicator in an object tile in the Active Directory Environment Overview to view summary information for the objects of that type in the selected alarm state.
- Select an object item from the Object Tree view (as described below) to view summary information for that individual object.

Description of embedded views

The Quick View consists of the following embedded views:

- [Object Tree view](#)
- [Object Summary View](#)
- [FAQs view](#)
- [Alarms view](#)

Object Tree view

The Object Tree view is located at the left of the Quick View and displays objects based on the tile selected in the Active Directory Environment Overview. Use the Object Tree view to select a single object or a group of objects of a particular type for display in the Object Summary view.

Object Summary View

The Object Summary view is located to the right of the Object Tree view and displays summary information for a single object or a group of objects, depending on what is selected in the Object Tree view.

The Object Summary view displays forest, server, site, and domain controller tiles (with the tile type reflecting the selected object type) or a number of embedded views which is determined by the item selected in the Active Directory Environment Overview and Object Tree view. A forest, server, site, or domain controller tile provides a quick and easy view into the items that make up the selected Active Directory® object and the alarm states of these items.

In addition, in the top right of the Overview Summary view there is a link to the Active Directory Explorer dashboard. This enables you to quickly navigate to the Active Directory Explorer for more detailed metrics about the selected object or group of objects.

The following table lists the information displayed when the different object tiles are selected.

Table 3. Object Summary view information


Item Selected in Overview	Item Selected in Object Tree	Views Displayed in Object Summary View
Forests Tile	Summary	A forest tile for each forest in your Active Directory environment.
Forests Tile - Alarm Indicator	Summary	A forest tile for each forest in the selected state.
Forests Tile or Alarm Indicator	Forest Item	In addition to a forest tile for the selected forest, the following embedded views are displayed: <ul style="list-style-type: none"> • Inventory By Category view • Statistics view • FSMO Roles view (Forest) • Trusts view • Top 3 Consumers view
Domains Tile	Summary	A domain tile for each domain in your Active Directory environment.
Domains Tile - Alarm Indicator	Summary	A domain tile for each domain in the selected state.
Domains Tile or Alarm Indicator	Domain Item	In addition to a domain tile for the selected domain, the following embedded views are displayed: <ul style="list-style-type: none"> • Inventory By Category view • Statistics view • FSMO Roles view (Domain) • Trusts view • Top 3 Consumers view
Sites Tile	Summary	A site tile for each site in your Active Directory environment.
Sites Tile - Alarm Indicator	Summary	A site tile for each site in the selected state.
Sites Tile or Alarm Indicator	Site Item	In addition to a site tile for the selected site, the following embedded views are displayed: <ul style="list-style-type: none"> • Inventory By Category view • IP Subnets view • Domain Controller Details view • Inter-Site Transports view • Top 3 CPU Consumers view
Domain Controllers Tile	Summary	A domain controller tile for each DC in your Active Directory environment.
Domain Controllers Tile - Alarm Indicator	Summary	A domain controller tile for each DC in the selected state.
Domain Controllers Tile or Alarm Indicator	Domain Controller Item	In addition to a domain controller tile for the selected DC, the following embedded views are displayed: <ul style="list-style-type: none"> • Host Monitor view • Agent State view • Server Health view • Top AD Metrics view

FAQts view

A FAQts view is displayed in the lower left corner of the Quick View on the Active Directory Environment dashboard and displays questions relating to the selected object. The questions in this view are scoped to the object tile selected in the Active Directory Environment Overview. For example, select the forest tile to view the questions about forests.

Figure 9. FAQts view



Use the **Previous** and **Next** buttons to scroll through the questions available for the selected object. Use the **Show Me** button to display the answer to the displayed question. Select the  button to display a list of all relevant questions from which to select.

Alarms view

The Alarms view that appears at the bottom of the Quick View in the Active Directory Environment dashboard displays a sortable list of all the outstanding alarms for the item selected in the Object Tree view.

i **NOTE:** An Alarms view also appears at the bottom of the Active Directory Explorer dashboard when you are viewing an object in the Active Directory Explorer Primary view (Summary navigation tab). It displays the outstanding alarms for the item selected in the Active Directory Enterprise view.

Active Directory Environment > CA Health Check tab

The CA Health Check tab provides you with an overview of your Certificate Authority (CA) environment being monitored, and includes the following metrics:

- **Server Name:** Displays the name of the monitored CA sever.
- **Issued Common Name:** Displays the “*Issued Common Name*”.
- **Expiration Date:** Indicates the date when the “*Issued Common Name*” will be expired.
- **Effective Date:** Indicates the date upon which the “*Issued Common Name*” is considered to take effect.
- **Days in Expire:** Indicates the period from now to the “*Issued Common Name*” expiration date. A minus indicates the “*Issued Common Name*” has been expired.

For more information about how to create a CA agent to be monitored, refer to [Add and configure a new Certificate Authority agent](#) on page 38.

i **NOTE:** Foglight for Active Directory only supports the monitoring of the environment installed with the Certificate Authority Enterprise Edition. Before creating a CA agent, click the **Script for configuring the Active Directory settings** link on the *Administration > Tasks* list to download and run a script that automatically configures the DCOM and WinRM. For more information, see the *readme.txt* file included in the script ZIP file.

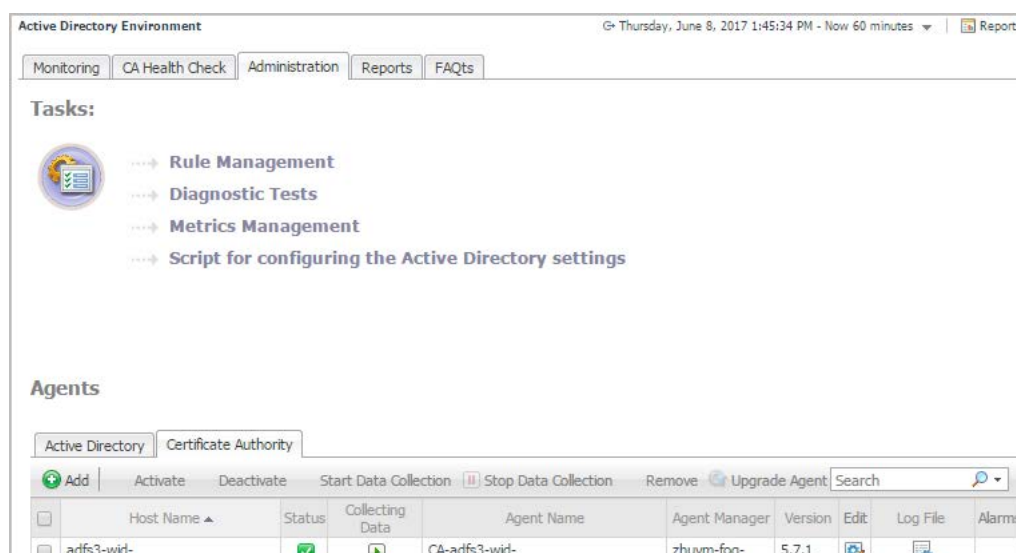
Active Directory Environment > Administration tab

The Administration tab includes the following components, and allows you to perform administrative tasks, as follows:

- Tasks list:
 - **Rule Management:** View and manage rules that exist in your environment. For more information, see [Foglight for Active Directory rules](#).
 - **Diagnostic Tests:** View a list of diagnostic tests that are available, as well as run a test immediately or define a schedule for when a test is to be run. For more information, see [Running diagnostic tests](#).
 - **Metrics Management:** View, edit, and enable/ disable the optional metric collections that are configurable for Active Directory agents. For more information, see [Managing Active Directory metrics](#).
 - **Script for configuring the Active Directory settings:** Download and run a script that automatically configures the Domain Controllers.
- Agents view:
 - **Certificate Authority:** Add and configure Certificate Authority agents on one or more servers. Once added, the Agent Management view displays all of the Certificate Authority agents configured to monitor CA metrics. For more information on using the Agent Setup wizard, see [Add and configure a new Certificate Authority agent](#).
 - **Active Directory:** Add and configure Active Directory agents on one or more DCs. Once added, the Agent Management view displays all of the Active Directory agents configured to monitor Active Directory metrics. For more information on using the Agent Setup wizard and the Agent Management view to manage your Active Directory agents, see [Managing Active Directory agents](#).

NOTE: In a federated environment, the administrative tasks and Agents view are available only on the Federated Children and not on the Foglight Federation Master.

Figure 10. Active Directory Environment > Administration tab

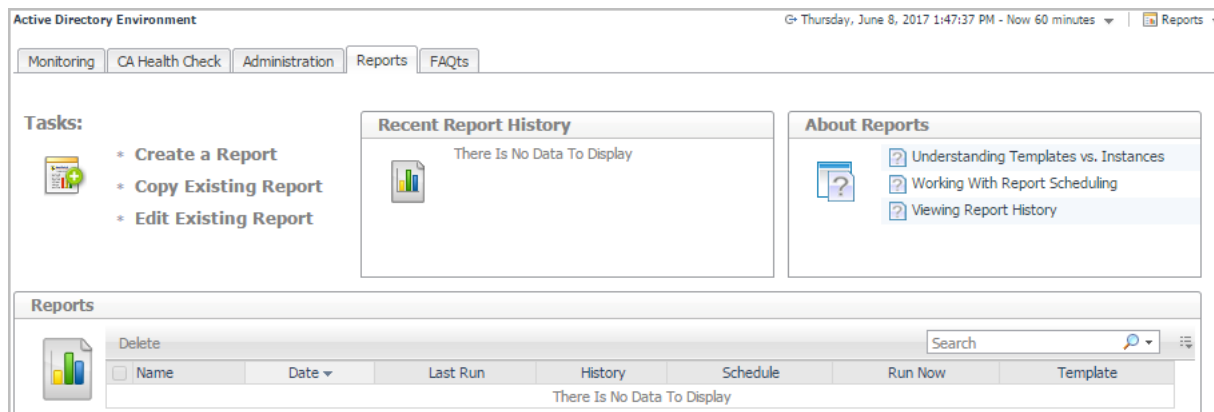


Active Directory Environment > Reports tab

The Reports tab allows you to manage custom Exchange reports. It consists of the following components:

- [Tasks list](#)
- [Recent Report History view](#)
- [About Reports view](#)
- [Reports view](#)

Figure 11. Active Directory Environment > Reports tab



Tasks list

From the Tasks list, you can create a report, copy an existing report, or edit an existing report for your Active Directory environment:

- Click **Create a Report** to select and generate a report using the [Create a Report wizard](#).
- Click **Copy Existing Report** to duplicate an existing report using the [Copy Existing Report wizard](#).
- Click **Edit Existing Report** to modify an existing report using the [Edit Existing Report wizard](#).

Create a Report wizard

To create a report:

- 1 Start the **Create a Report** wizard.
- 2 On the **Basic Configuration** page, define the following settings, then click **Next**:
 - **Scheduled Report Name**: Type a valid name for the report.
 - **Report Templates**: Select the template on which you want to base your report. The Report Inputs section is populated with the template's report parameters. Use the default parameters to quickly create a report, or optionally change the report parameters to customize the report to better meet your requirements. For more details about Active Directory template reports, see [Foglight for Active Directory reports](#).
- 3 On the **Advanced Configuration** page, define the following settings, then click **Finish**:
 - **Schedule**: Select the report schedule from the list of available options.
 - **Retained Results**: Type the number of results retained for the report.
 - **Enabled**: Select the check box if you want to enable the report. Clear the check box if you want to disable the report.
 - **Report Format**: Select the report format from the list of available options.
 - **Email Recipients**: Type the email addresses of the recipients to be notified when the report is generated.

The scheduled report is created and appears in the Reports view.

Copy Existing Report wizard

To copy an existing report:

- 1 Start the **Copy Existing Report** wizard.
- 2 On the **Select Report** page, select the report to be copied, then click **Next**.
- 3 On the **Edit Report Configuration** page, define the following settings, then click **Finish**:
 - **Scheduled Report Name**: Type a valid name for the new report.
 - **Report Templates**: The report template can not be modified, only the report parameters in the Report Inputs section at the bottom of the page.
 - **Schedule**: Select the report schedule from the list of available options.
 - **Retained Results**: Type the number of results retained for the report.
 - **Enabled**: Select the check box if you want to enable the report. Clear the check box if you want to disable the report.
 - **Report Format**: Select the report format from the list of available options.
 - **Email Recipients**: Type the email addresses of the recipients to be notified when the report is generated.

The scheduled report is created and appears in the Reports view.

Edit Existing Report wizard

To edit an existing report:

- 1 Start the **Edit Existing Report** wizard.
- 2 On the **Select Report** page, select the report to be edited, then click **Next**.
- 3 On the **Edit Current Configurations** page, define the following settings, then click **Finish**:
 - **Scheduled Report Name**: Change the report name, as necessary.
 - **Report Templates**: The report template and its parameters can not be modified.
 - **Schedule**: Select the report schedule from the list of available options.
 - **Retained Results**: Type the number of results retained for the report.
 - **Enabled**: Select the check box if you want to enable the report. Clear the check box if you want to disable the report.
 - **Report Format**: Select the report format from the list of available options.
 - **Email Recipients**: Type the email addresses of the recipients to be notified when the report is generated.

The new report settings are saved and the updated scheduled report appears in the Reports view.

Recent Report History view

The Recent Report History view provides information about the most recent report instances run in your environment.

About Reports view

The About Reports view enables you to get answers to common questions about Active Directory reports.


Clicking a question from the list displays a dialog box that provides information about the selected topic.

Reports view

The Reports view displays all of the report instances configured in your Active Directory environment.

The view contains the following information for each configured report instance.

Table 4. Reports view - information

Column	Description
	Use the selection check boxes to select report instances for running or removal.
Name	Displays the name of the report.
Date	Indicates the date and time when the report was last run.
Last Run	Indicates the report type.
History	Click the icon in this column to open the Report History dialog box, and review the history of the selected report. To view the report content, click one item in the list.
Schedule	Displays the time when the report is scheduled to run.
Run Now	Click the icon in this column to manually run a selected report. The Run Now dialog box opens, displaying the status of the report generation. When the report is complete, you can view the report content by clicking the Download .
Template	Displays the template used for a scheduled report.

To delete one or several reports from the list, select the report(s) and click the **Delete** button at the top left corner of the view.

To search for a particular report, type the report name on the **Search** box at the top right corner of the view, then click **Enter**.

Active Directory Environment > FAQs tab

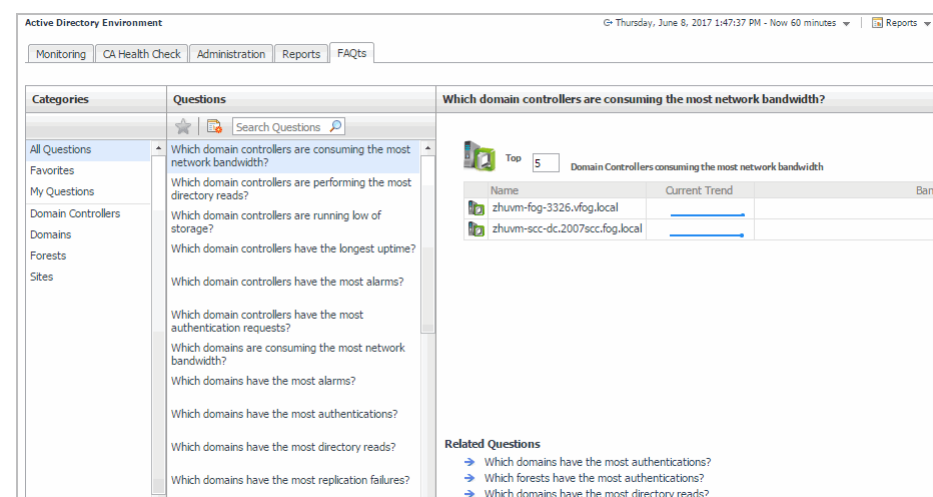
In addition to the FAQs embedded view in the Quick View, a FAQs view appears as a navigation tab at the top of the dashboard. The FAQs navigation tab provides a list of all the questions available for all Active Directory® object types.

i | **NOTE:** The FAQs navigation tab is also available in the Active Directory Explorer dashboard when you are viewing an object in the Active Directory Explorer Primary view.

Purpose

The FAQs view enables you to get answers to common questions about your Active Directory® environment.

Figure 12. FAQs view - navigation tab



Description of embedded views

The FAQs navigation tab is made up of the following embedded views:

- [Categories view](#)
- [Questions view](#)
- [Answer view](#)

Categories view

The Categories view lists the categories (that is, forests, domains, sites or domain controllers) for which questions can be answered by Foglight. It also contains a **Favorites** and **My Questions** category which allows you to customize the list of questions displayed.

By default, **All Questions** is selected. Click a category to view a list of questions relating to a type of Active Directory® object or click **Favorites** or **My Questions** to view your customized list of questions.



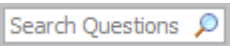


Questions view

The Questions view lists the questions available for the category selected in the Categories view.

Click a question from the list to have Foglight gather and report an answer.

Use the buttons at the top of the Questions view as follows.

Table 5. Questions view

	Mark the selected question as a 'favorite'. Questions marked as a 'favorite' will be displayed when the Favorites category is selected.
	Create a report based on selected questions.
	If the list of questions is long, you can narrow it down by entering a text string in the Search field. Enter a word or text string and select the search button  to display only those questions that contain the word or string entered. To clear the filter and return to the original list of questions, click  .

Answer view

The Answer view provides an answer to the question selected in the Questions view. The answer is provided in the following form:

Top x <objects of category> ...

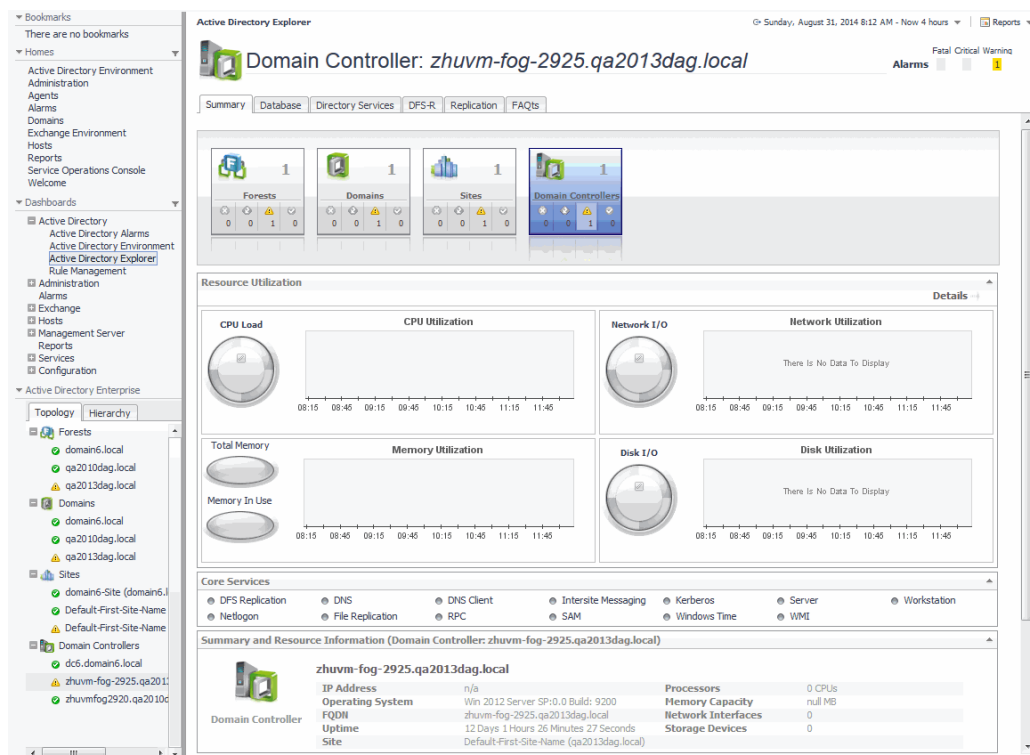
where x is the number of objects of the category selected in the Categories view.

It also lists related questions from which you can select. Selecting a related question will refresh the Answer view displaying the answer to the selected question.

Active Directory Explorer dashboard

The Active Directory Explorer dashboard has a hierarchal interface that you can use to view various performance metrics and alarms within your Active Directory® infrastructure. It provides informative views through which you can quickly and easily access detailed information about any of the objects in your Active Directory environment.

Figure 13. Active Directory Explorer dashboard

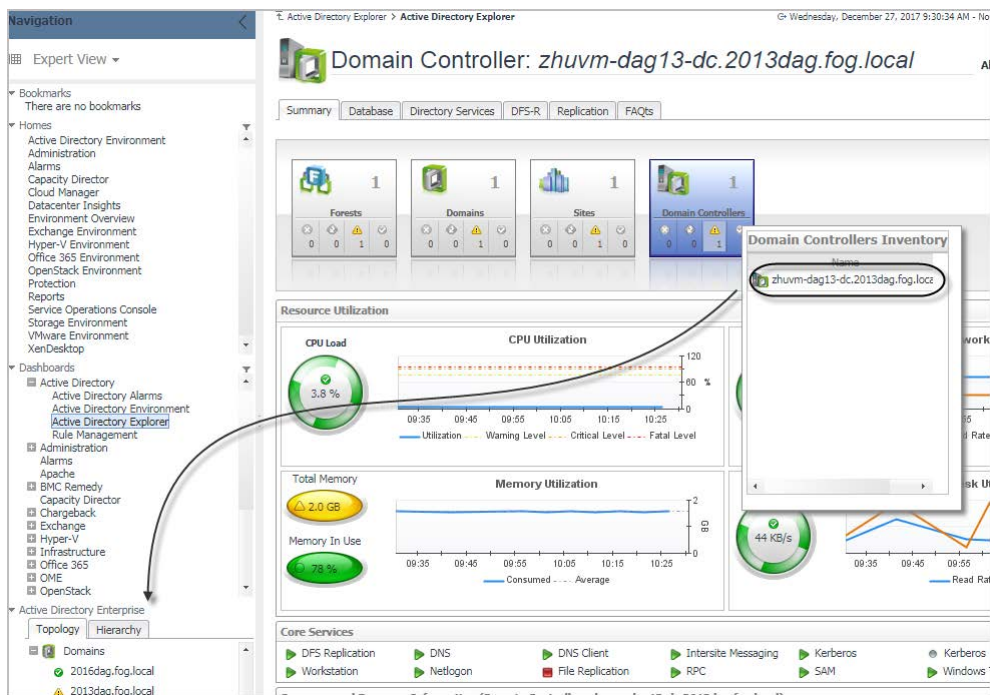


The Active Directory Explorer dashboard contains the following views:

- [Active Directory Enterprise view](#)
- [Active Directory Explorer Primary view](#)

Active Directory Enterprise view

After choosing an object from the *Domain Controllers Inventory* tile, the Active Directory Enterprise view appears in the navigation panel, under the *Dashboards* list.



Purpose

The Active Directory Enterprise view provides an organized view of the Active Directory® objects that are monitored by the Foglight for Active Directory.

Clicking an object type container or object in the Active Directory Enterprise view refreshes all of the views in the Active Directory Explorer Primary view to display information pertaining to the selected object.

Description of embedded views

The Active Directory Enterprise view is made up of the following embedded views:

- [Topology view](#)
- [Hierarchy view](#)
- [Mouse-over status popup](#)

Use these views to display performance metrics and alarms for an individual Active Directory® object or group of objects of a particular type.

Topology view

The Topology view is organized into a tree using object type containers for branches. The top-level containers are the main Active Directory object types (that is, forests, domains, sites, and domain controllers) and each object type container contains every object of that particular type that is managed by the cartridge. Click the expansion state box to the left of a container to expand the view to display the individual objects.

To the left of each object, a status indicator represents the alarm of highest severity that is outstanding for that object.

Hierarchy view

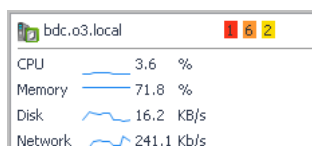
The Hierarchy view represents the logical layout of the containers in your Active Directory environment. In the Hierarchy view, each forest container is organized into a tree illustrating where each domain and domain controller resides within your Active Directory environment. Click on the expansion state box to the left of a container to expand the view to display subordinate objects.

To the left of each object, a status indicator represents the alarm of highest severity that is outstanding for that object.

Mouse-over status popup

When you hover the cursor over an object in the Active Directory Enterprise view, a popup appears that provides a summary of the present state of the selected object. For example, the following popup appears when you hover the cursor over an individual DC object in the Active Directory Enterprise view.

Figure 14. Status popup



Active Directory Explorer Primary view

The Active Directory Explorer has a Primary view which takes up the entire display panel of the browser interface. This view displays information based on the object type container or object selected in the Active Directory Enterprise view.

Purpose

The Active Directory Explorer Primary view displays performance metrics and alarms related to the objects within an object type container or an individual Active Directory® object.

The heading area located across the top of the Active Directory Explorer Primary view consists of the following main components:

- an object icon and name
- an alarm summary for the selected object type container or object
- navigation tabs

The object icon and name to the left of the heading specify the object type container or individual object that is selected in the Active Directory Enterprise view.

The alarm summary at the right of the heading shows you the number of alarms at each severity level that are outstanding for the selected object. Clicking an alarm count displays a popup that lists the active alarms for the object. From this popup you can display additional details about an individual alarm.

The navigation tabs are located immediately below the selected object's name. These navigation tabs vary from object to object, but generally contain an object summary tab, a FAQs tab, and one or more tabs of other relevant information. The following table lists the navigation tabs displayed based on the item selected in the Active Directory Enterprise view.

Table 6. Active Directory Explorer Primary view information

Item Selected in Active Directory Enterprise View	Tabs Displayed in Active Directory Explorer Primary View
Object Container (Forests, Domains, Sites, or Domain Controllers)	<ul style="list-style-type: none"> • Summary (All) • FAQs
Forest Object	<ul style="list-style-type: none"> • Summary • FAQs
Domain Object	<ul style="list-style-type: none"> • Summary • FAQs

Table 6. Active Directory Explorer Primary view information

Item Selected in Active Directory Enterprise View	Tabs Displayed in Active Directory Explorer Primary View
Site Object	<ul style="list-style-type: none"> • Summary • FAQs
Domain Controller Object	<ul style="list-style-type: none"> • Summary • Database • Directory Services • FRS / DFS-R • Replication • FAQs

Description of embedded views

The Primary view changes in appearance and content, depending on which navigation tab is selected. The metrics and amount of detail displayed varies depending on the type of object you selected in the Active Directory Enterprise view.

The Primary view may contain the following embedded views:

- [Domain Controller - Summary view](#)
- [Domain Controller - Database view](#)
- [Domain Controller - Directory Services view](#)
- [Domain Controller - FRS / DFS-R view](#)
- [Domain Controller - Replication view](#)
- [Domain Controller - FAQs view](#)

Domain Controller - Summary view

Selecting the **Summary** navigation tab displays the Summary view just below the heading. This view provides a hierarchical inventory, in the form of tiles, of the objects that are related to the object or object container selected in the Active Directory Enterprise view. Each tile shows how many objects of the corresponding object type there are, as well as the count of objects of that type in each of the alarm states (fatal, critical, warning, and normal).

On a tile, click the object type icon, the object type name, or the object count, to view an inventory popup that lists all objects of the corresponding type, along with their respective states. Click an object in the inventory popup to view details for that object in the Active Directory Explorer Primary Summary view.

On a tile, click an alarm state or the number below it to view an alarms popup that shows the outstanding alarms of that state for the corresponding object type. Click an alarm in the alarms popup to view details about the selected alarm.

i **NOTE:** If the alarm state has a count of zero, you cannot select that alarm state. When you click a normal state icon or count, the Active Directory Explorer page is refreshed, but you do not see the alarms popup because there are no alarms associated with the normal state.

More detailed information associated with the object or object container selected in the Active Directory Enterprise view is displayed in views below the Summary view. The following table lists the embedded views displayed when the different objects or object containers are selected.

Table 7. Embedded views in Summary view

Item Selected in Active Directory Enterprise View	Embedded Views in Summary View
Object Container (Forests, Domains, Sites, or Domain Controllers)	<ul style="list-style-type: none"> • Top 3 CPU Consumers • Top 3 Memory Consumers • Top 3 Network Consumers • Top 3 Storage Consumers • Domain Controllers • Alarms
Forest, Domain or Site Object	<ul style="list-style-type: none"> • Top 3 DS Directory Reads • Top 3 LDAP Bind Times • Top 3 Replication Queue Length • Top 3 CPU Consumers • Top 3 Memory Consumers • Top 3 Network Consumers • Top 3 Storage Consumers • Domain Controllers • Alarms
Domain Controller Object	<ul style="list-style-type: none"> • Resource Utilization • Core Services • Summary and Resource Information • Alarms

Domain Controller - Database view

When an individual domain controller is selected in the Active Directory Enterprise view, a Database navigation tab appears. Selecting the **Database** navigation tab displays the Domain Controller Database view. By default, this view consists of database performance metrics associated with the selected DC. Additional database metrics can optionally be displayed by enabling the corresponding collection group on the Active Directory Metrics Management dashboard.

Domain Controller - Directory Services view

When an individual domain controller is selected in the Active Directory Enterprise view, a Directory Services navigation tab appears. Selecting the **Directory Services** navigation tab displays the Domain Controller Directory Services view. By default, this view consists of directory service related performance metrics associated with the selected DC. Additional directory services metrics can optionally be displayed by enabling the corresponding collection group on the Active Directory Metrics Management dashboard.

Domain Controller - FRS / DFS-R view

When an individual domain controller is selected in the Active Directory Enterprise view, either an FRS or a DFS-R navigation tab will be present, depending on the file replication service set up for the SYSVOL on the selected DC.

- Selecting the **FRS** navigation tab displays the Domain Controller FRS view. By default, this view consists of File Service Replication (FRS) related performance metrics associated with the SYSVOL on the selected DC. Additional file service replication metrics can optionally be displayed by enabling the corresponding collection group on the Active Directory Metrics Management dashboard.
- Selecting the **DFS-R** navigation tab displays the Domain Controller DFS-R view. By default, this view consists of Distributed File System Replication (DFS-R) service performance metrics associated with the SYSVOL on the selected DC. Additional DFS replication service metrics can optionally be displayed by enabling the corresponding collection group on the Active Directory Metrics Management dashboard.

Domain Controller - Replication view

When an individual domain controller is selected in the Active Directory Enterprise view, a Replication navigation tab appears. Selecting the **Replication** navigation tab displays the Domain Controller Replication view. By default, this view consists of replication performance metrics associated with the selected DC. Additional replication metrics can optionally be displayed by enabling the corresponding collection group on the Active Directory Metrics Management dashboard.

Domain Controller - FAQs view

Selecting the **FAQs** navigation tab displays a list of all the questions available for all Active Directory® objects.

NOTE: The FAQs navigation tab is also available in the Active Directory Environment dashboard. See [Active Directory Environment > FAQs tab](#) for more information.

Active Directory Rule Management dashboard

The Active Directory Rule Management dashboard contains a sortable list of the conditional severity rules used by the Foglight for Active Directory. From this dashboard you can quickly see which conditional rules are enabled/disabled, the states (fatal, critical or warning) with active conditions, predefined alarm threshold values, rules with current alarms, and a brief description of each rule.

Figure 15. Active Directory Rule Management dashboard

Enabled	Rule	Alarms	Description
<input type="checkbox"/>	Host Logical Disk Sec: Average Read	1000	Checks if the logical disk average read time (in ms) is above the threshold.
<input type="checkbox"/>	Host Logical Disk Sec: Average Write	1000	Checks if the logical disk average write time (in ms) is above the threshold.
<input type="checkbox"/>	Host Physical Disk Sec: Average Read	1000	Checks if the physical disk average read time (in ms) is above the threshold.
<input type="checkbox"/>	Host Physical Disk Sec: Average Write	1000	Checks if the physical disk average write time (in ms) is above the threshold.
<input type="checkbox"/>	LDAP Bind Time	400	LDAP Bind Time rule.
<input type="checkbox"/>	Global Catalog Demotion	2	Monitoring of domain controllers for the demotion of Global Catalog status.
<input type="checkbox"/>	Global Catalog Promotion	2	Monitoring of domain controllers as they promote to Global Catalog status.
<input type="checkbox"/>	Host CPU Utilization SdDev	2	Checks for spikes or dramatic drops in CPU Utilization on a server.
<input type="checkbox"/>	Host Disk IO	2	Checks for spikes or dramatic drops in Disk IO on a server.
<input type="checkbox"/>	Host DOT NET Framework Memory	2	Checks if the percentage of time in garbage collection (GC) is above the threshold.
<input type="checkbox"/>	Host Logical Disk Capacity Available	2	Monitors the value of the 'Capacity Available' metric, as it diminishes.
<input type="checkbox"/>	Host Memory Available	1	Checks if the memory usage is above the threshold value.
<input type="checkbox"/>	Host Memory Cached	3	Checks if the memory cached is abnormally high based on previous and current values.
<input type="checkbox"/>	Host Memory Paging	2	Checks if the sum of the page in rate and the page out rate is above the threshold.
<input type="checkbox"/>	Host Memory Percent Committed	5	Checks if the percentage of memory committed bytes is above the threshold.
<input type="checkbox"/>	Host Memory Pool Non-Paged Bytes	2	Checks if the memory pool non-paged bytes is abnormally high based on previous and current values.
<input type="checkbox"/>	Host Memory Pool Paged Bytes	2	Checks if the memory pool paged bytes is abnormally high based on previous and current values.
<input type="checkbox"/>	Host Memory Utilization	2	Host Memory Utilization.
<input type="checkbox"/>	Host Memory Utilization SdDev	2	Checks for spikes or dramatic drops in Memory Utilization on a server.
<input type="checkbox"/>	Host Network Available Bandwidth	2	Checks if the available network bandwidth is less than the threshold value.
<input type="checkbox"/>	Host Network IO	2	Checks for spikes or dramatic drops in Network IO on a server.
<input type="checkbox"/>	Host Processor Queue Length	2	Checks if the processor queue length is above the threshold value.
<input type="checkbox"/>	Host Storage Capacity	2	Checks if at the present growth rate the logical drive will be full within the threshold.
<input type="checkbox"/>	Active Directory Host Services	4	Active Directory Host Services.
<input type="checkbox"/>	ESE Database Cache Percent Hit	2	ESE Database Cache Percent Hit rule.
<input type="checkbox"/>	ESE Database Cache Size	2	ESE Database Cache Size rule.

For a description of the Active Directory Rule Management dashboard and for more information on the Foglight for Active Directory rules and how to enable, disable or modify them, see [Foglight for Active Directory rules](#).

Managing Active Directory agents

The Active Directory agents collect data from remote Active Directory® domain controllers, which is then used to populate the health and performance metrics presented throughout Foglight for Active Directory dashboards and views.

The Foglight for Active Directory provides an additional dashboard that can be used to manage Active Directory agent instances. Therefore, the Active Directory agent instances can be created and managed using one of the following dashboards:

- Agent Status dashboard (**Dashboards > Administration > Agents > Agent Status**)
- Active Directory Environment dashboard > Administration tab (**Dashboards > Active Directory Environment > Administration tab**)

This section describes the Deploy Agent Package dialog, Agent Setup wizard which is used to add and configure new Active Directory agents and the Agent Management view which is populated with information about each Active Directory agent instance. It also provides a description of the Active Directory agent properties used to connect to the target server from which data is to be collected.

- [Agent Status dashboard](#)
- [Active Directory/Certificate Authority agent management](#)
- [Active Directory agent properties](#)

Agent Status dashboard

The Agent Status dashboard allows you to deploy agent packages and create agent instances one host at a time. Once an agent is created, use this dashboard to view agent information and edit the properties of one or more agents.

For more information about using the Agent Status dashboard to create and manage agent instances, see “Deploying agent packages to monitored hosts” in the *Foglight Administration and Configuration Help*.

Active Directory/Certificate Authority agent management

The *Active Directory Environment dashboard > Administration* tab allows you to create agent instances for one or more servers at a time, activate or deactivate Active Directory agents or Certificate Authority agents, and start and stop collecting data.

The Administration tab consists of the following components:

- [Tasks list](#)
- [Agent Management view](#)

Tasks list

The Tasks list, in the upper left corner of the view, contains a list of tasks that can be performed from this view.

Figure 16. Task list



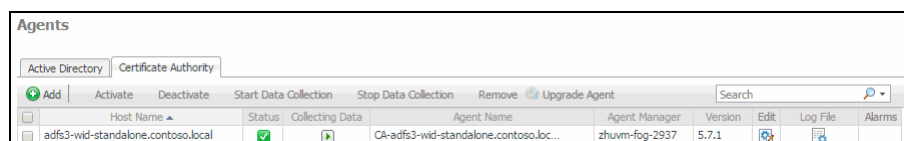
Clicking the **Script for configuring the Active Directory settings** link on this list downloads and runs a script that automatically configures the Domain Controllers and WinRM. For more information, see the *readme.txt* file included in the script ZIP file.

Agent Management view

Once Active Directory® agent or Certificate Authority agents are added, the Agent Management list displays all of the agent instances configured to monitor metrics.

NOTE: In a federated environment, the administrative tasks and Agents view are available only on the Federated Children and not on the Foglight Federation Master.

Figure 17. Agent Management view



The Agent Management view contains the following information for each configured Active Directory or Certificate Authority agent instance.

Table 8. Agent Management view - information


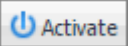
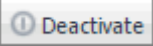
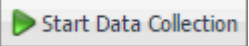
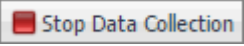
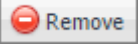
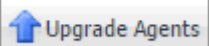
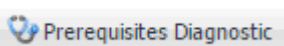

Column	Description
	Use the selection check boxes to select agent instances for activation/deactivation, starting/stopping data collection, editing properties, or removal.
Domain Controller (Active Directory only)	Displays the name of the DCs being monitored by an Active Directory agent instance.
Host Name (Certificate Authority only)	Displays the name of the server being monitored by a Certificate Authority agent instance.
Status	Indicates whether the agent instance for a Domain Controller or a Host is activated. A green check mark in this check box indicates that the agent is active.
Collecting Data	Indicates whether the agent instance is currently collecting data. A green check mark in this check box indicates that the agent is collecting data.
Agent Name	Displays the name of the agent instance created for a DC or a host.
Agent Manager	Displays the name of the Foglight Agent Manager Host assigned to each agent instance.
Edit	Click the icon in this column to update agent properties using the Agent Edit wizard. For more information, see Edit private agent properties on page 39.

Table 8. Agent Management view - information

Column	Description
Log File	Click the icon in this column to download the agent log.
Version	Displays the agent version. A green check mark icon indicates that the agent version is up to date.
Alarms	Displays the number of alarms occurred on each agent instance.

Use the buttons at the top of this list to manage your Active Directory or Certificate Authority agent instances, as described in the following table.

Table 9. Agent Management view - buttons

Button	Description
	Select to launch the Agent Setup wizard to add and configure new Active Directory agent instances. For more information, see Add and configure new Active Directory agents .
	Select to activate the selected agent instance(s).
	Select to deactivate the selected agent instance(s).
	Select to start collecting data on the selected agent instance(s).
	Select to stop collecting data on the selected agent instance(s).
	Select to remove the selected agent instance(s).
	Create and assign credentials for an Active Directory agent created before version 5.6.6.
	Verify agent configuration. For more information, see Inspect agent prerequisites . NOTE: This button is only available in the <i>Agents > Active Directory</i> tab.
	Search for an Active Directory agent using the Search filter.

Add and configure new Active Directory agents

The Agent Setup wizard steps you through the process of adding and configuring Active Directory® agent instances on one of more Domain Controllers (DCs).

To add and configure a new agent:

- 1 At the top of the Agent Management view, click **Active Directory**, and then click **Add** to launch the Agent Setup wizard.
- 2 On the **Prepare** page, carefully read the instructions about the steps that you need to take before proceeding with the wizard.

You can either manually configure your Active Directory environment for monitoring, or download and run a script that automatically configures the Domain Controllers. To download the script, click **Script for configuring the Active Directory settings**.

When done, click **Next**.

- 3 On the **Auto-Discovery or Manual** page, indicate if you want to manually configure an Active Directory agent to monitor a single Domain Controller, or search your domain and auto-discover Domain Controllers via LDAP. Click **Next**.
 - If you selected **Auto-discover**, continue with [Step 4](#).
 - If you selected **Manual**, continue with [Step 6](#).
- 4 On the **Select the Search Domain** page, specify the domain to search for Domain Controllers, where Active Directory agent instances are to be created and activated.
 - **Domain:** Type the fully qualified name (*myDomain.com*) of a domain to search for Domain Controllers (DCs).
 - **User Name:** Type the user principal name of the account to be used to query Active Directory® on the selected domain. The following formats are accepted for the user principal name: *myUser@myDomain.com*, *myUser*, and *myDomain.com\myUser*.
 - **Password:** Enter the password associated with the above user account.
 - **Enable SSL For LDAP:** Selecting this check box if security LDAP is required.

Click **Next**.

i NOTE:

1. When selecting **Enable SSL For LDAP**, import the root certificate of the monitoring domain into both FglAM and Foglight keystore.
 2. Ensure that the Subject Alternative Name of the certificate used by LDAP service includes both server FQDN and Domain name.
- For detailed information on how to import certificate into both FMS and FglAM keystore in FIPS-compliant mode, refer to [Managing certificates for FglAM on page 42](#) and [Managing certificates for FMS in FIPS-compliant mode on page 45](#).
- For detailed information on how to import certificate into both FMS and FglAM keystore in non-FIPS mode, refer to [Managing certificates for FglAM on page 42](#) and [Managing certificates for FMS in non-FIPS mode on page 44](#).

- 5 On the **Select Servers** page, select one or more DCs that you want to monitor.

i NOTE: All selected servers will use the same user credentials for access.

This page displays the following information for each DC found on the selected domain:

- **Domain Controller:** Displays the name of the DCs found on the selected domain.
- **Active Directory Agent Exists:** Indicates whether an Active Directory agent instance has already been created for a DC. A green check mark in this check box indicates that an agent instance has already been created for the DC. DCs already monitored by other Active Directory agents are unavailable for selection in the list.

Click **Next**.

- 6 On the Configure **Agent Properties** page, review the Active Directory agent properties, and edit them, as necessary. select the agent properties, as necessary.
 - **Domain Controller(s):** The name of the domain controller found on the selected domain.
 - **Communication Protocol:** Selects to run the WMI query through DCOM or WinRM.
 - **WinRM Port:** The WinRM port number on the monitored Domain Controller. This property only appears if the **Communication Protocol** is set to **WinRM through HTTP** or **WinRM through HTTPS**.

i NOTE:

1. When setting **Communication Protocol** as **WinRM through HTTPS**, import the root certificate of the monitoring domain into FglAM keystore.
 2. Ensure that the Subject Alternative Name of the certificate used by LDAP service includes both server FQDN and Domain name.
- For detailed information on how to import certificate into FglAM keystore, refer to [Managing certificates for FglAM on page 42](#).

- **LDAP Authentication Mechanism:** The authentication scheme used to connect to the LDAP server: **Simple** (default) or **Kerberos**.
- **Enable SSL For LDAP:** Indicates if the LDAP connection is secure or not (default).

i NOTE:

1. When selecting **Enable SSL For LDAP**, import the root certificate of the monitoring domain into both FglAM and Foglight keystore.
2. Ensure that the Subject Alternative Name of the certificate used by LDAP service includes both server FQDN and Domain name.

For detailed information on how to import certificate into both FMS and FglAM keystore in FIPS-compliant mode, refer to [Managing certificates for FglAM](#) on page 42 and [Managing certificates for FMS in FIPS-compliant mode](#) on page 45.

For detailed information on how to import certificate into both FMS and FglAM keystore in non-FIPS mode, refer to [Managing certificates for FglAM](#) on page 42 and [Managing certificates for FMS in non-FIPS mode](#) on page 44.

- **Is a Virtual Host?:** Indicates if the selected Domain Controller runs on a virtual host.
- **Virtual Environment:** The type of the virtual environment: **VMware** or **Hyper-V**. This property only appears if the selected Domain Controller runs on a virtual host.

- 7 On the **Select the Agent Manager Host** page, select the Foglight Agent Manager Host to be used for the new Active Directory agent instances.

The table displays the following Foglight Agent Manager information (same information is displayed on the Administration > Agents > Agent Hosts dashboard):

- Host Name
- Agent Manager Version
- OS Type
- OS Architecture
- The **Active Directory Agent Package Deployed** column indicates whether the Active Directory agent package has been deployed to the Foglight Agent Manager host(s). A green check in this column indicates that the Active Directory agent package has been deployed.

i NOTE: This value is not aware of a package's version. Therefore, if you have upgraded the cartridge, you must deploy the new agent package even if this column indicates that the FglAM host already has an agent package.

- The **Windows Agent Package Deployed** column indicates whether the Windows agent package is already deployed to the Agent Manager host(s). A green check in this column indicates that the Windows agent package has been deployed. This column is displayed only if the selected Domain Controller runs on a physical host.

Click **Next**.

- 8 On the **Assign and Validate Credentials** page, review the available credentials, and edit them, as necessary.

- To create a new credential, click **Add host(s) to a new credential**.
 - In the **Create New Credential and Assign** dialog box, create a credential that you want to use to access the monitored resource. Type a new credential name, domain, user name, password, and lockbox, and click **Submit**.
- To select an existing credential, click **Add host(s) to an existing credential**.
 - In the **Select Existing Credential** dialog box, select an existing credential, and click **Submit**.
- To bypass the prerequisites verification, select the **Do not check for prerequisites** check box.

Click **Next**.

- 9 On the **Summary** page, review the configuration settings chosen for the new agent, and its prerequisite diagnostics, including:

- **Active Directory Agent:** The name of the selected Active Directory agent instance.
- **Windows Agent:** The name of the selected Windows agent instance.
- **Diagnostic Result:**

i | **NOTE:** This information is displayed only when the prerequisites are checked in [Step 8](#).

- **Success:** The agent instance can connect to the monitored Domain Controller and collect data.
- **Error:** The agent instance cannot connect to the monitored Domain Controller instance and collect data. Click this link to find out what causes this error. Carefully review the information in the popup that appears in order address the problem.

Click **Finish**.

The Agent Setup wizard closes. The Active Directory agent is now added and configured, and appears in the Agent Management view, on the *Administration > Active Directory* tab.

Add and configure a new Certificate Authority agent

The Agent Setup wizard steps you through the process of adding and configuring Certificate Authority agent instances on one of more host servers.

i | **NOTE:**

- Foglight for Active Directory only supports the monitoring of the environment installed with the Certificate Authority Enterprise Edition. Before creating a CA agent, click the **Script for configuring the Active Directory settings** link on the *Administration > Tasks* list to download and run a script that automatically configures the DCOM and WinRM. For more information, see the *readme.txt* file included in the script ZIP file.
- To run remote scripts, a **Certificate Authority** agent requires an account with relevant privileges:
 - If the Certificate Authority server is a member server then agent account needs to be member of *Domain Admins* group.
 - If the Certificate Authority is a Domain Controller then the agent account needs to be member of either *Domain Administrators* group or *Domain Admins* group.

To add and configure a new certificate authority agent:

- 1 At the top of the Agent Management view, click **Certificate Authority**, and then click **Add** to launch the Agent Setup wizard.
- 2 On the **Configure CA Agent Properties** page, specify the host where Certificate Authority agent instances are to be created and activated.
 - **Host Name:** Type the fully qualified name of a Certificate Authority server.
 - **Communication Protocol:** Selects to run the WMI query through DCOM or WinRM.
 - **WinRM Port:** The WinRM port number on the monitored Host. This property only appears if the **Communication Protocol** is set to **WinRM through HTTP** or **WinRM through HTTPS**.

i | **NOTE:**

1. When setting **Communication Protocol** as **WinRM through HTTPS**, import the root certificate of the monitoring domain into FglAM keystore.
2. Ensure that the Subject Alternative Name of the certificate used by LDAP service includes both server FQDN and Domain name.

For detailed information on how to import certificate into FglAM keystore, refer to [Managing certificates for FglAM](#) on page 42.

Click **Next**.

- 3 On the **Select the Agent Manager Host** page, select the Foglight Agent Manager Host to be used for the new Certificate Authority agent instances.

The table displays the following Foglight Agent Manager information (same information is displayed on the Administration > Agents > Agent Hosts dashboard):

- Host Name
- Agent Manager Version
- OS Type
- OS Architecture
- The **Certificate Authority Agent Package Deployed** column indicates whether the Certificate Authority agent package has been deployed to the Foglight Agent Manager host(s). A green check in this column indicates that the Certificate Authority agent package has been deployed.

i NOTE: This value is not aware of a package's version. Therefore, if you have upgraded the cartridge, you must deploy the new agent package even if this column indicates that the FglAM host already has an agent package.

Click **Next**.

- 4 On the **Assign and Validate Credentials** page, review the available credentials, and edit them, as necessary.
 - To create a new credential, click **Add host(s) to a new credential**.
 - In the **Create New Credential** dialog box, create a credential that you want to use to access the monitored resource. Type a new credential name, domain, user name, password, and lockbox, and click **Submit**.
 - To select an existing credential, click **Add host(s) to an existing credential**.
 - In the **Assign Credential** dialog box, select an existing credential, and click **Assign**.

Click **Next**.

- 5 On the **CA Summary** page, review the configuration settings chosen for the new agent, and its prerequisite diagnostics, including:
 - **Host Name:** The name of the selected Certificate Authority agent instance.
 - **Communication Protocol:** The communication protocol selected to run the WMI query.
 - **WinRM Port:** The WinRM port number on the monitored Host. This property only appears if the **Communication Protocol** is set to **WinRM through HTTP** or **WinRM through HTTPS**.
 - **Agent Manager:** The name of the selected Foglight Agent Manager Host to be used for the new Certificate Authority agent instances.

Click **Finish**.

The Agent Setup wizard closes. The Certificate Authority agent is now added and configured, and appears in the Agent Management view, on the *Administration > Certificate Authority* tab.

Edit private agent properties

The **Agent Edit** wizard guides you through the process of editing private agent properties.

To edit private agent properties:

- 1 In the Agent Management view, in the row containing the agent whose properties you want to edit, click the **Edit** column.
- 2 In the **Agent Edit** wizard, on the **Configure Agent Properties** page, review the Active Directory agent properties, and edit them, as necessary.
 - **Domain Controller(s):** The name of the domain controller found on the selected domain.

- **Communication Protocol:** Selects to run the WMI query through DCOM or WinRM.
- **WinRM Port:** The WinRM port number on the monitored Domain Controller. This property only appears if the **Communication Protocol** is set to **WinRM through HTTP** or **WinRM through HTTPS**.



NOTE:

1. When setting **Communication Protocol** as **WinRM through HTTPS**, import the root certificate of the monitoring domain into FglAM keystore.
 2. Ensure that the Subject Alternative Name of the certificate used by LDAP service includes both server FQDN and Domain name.
- For detailed information on how to import certificate into FglAM keystore, refer to [Managing certificates for FglAM](#) on page 42.

- **LDAP Authentication Mechanism:** The authentication scheme used to connect to the LDAP server: **Simple** (default) or **Kerberos**.
- **Enable SSL For LDAP:** Indicates if the LDAP connection is secure or not (default).



NOTE:

1. When selecting **Enable SSL For LDAP**, import the root certificate of the monitoring domain into both FglAM and Foglight keystore.
 2. Ensure that the Subject Alternative Name of the certificate used by LDAP service includes both server FQDN and Domain name.
- For detailed information on how to import certificate into both FMS and FglAM keystore in FIPS-compliant mode, refer to [Managing certificates for FglAM](#) on page 42 and [Managing certificates for FMS in FIPS-compliant mode](#) on page 45.
- For detailed information on how to import certificate into both FMS and FglAM keystore in non-FIPS mode, refer to [Managing certificates for FglAM](#) on page 42 and [Managing certificates for FMS in non-FIPS mode](#) on page 44.

- **Is a Virtual Host?:** Indicates if the selected Domain Controller runs on a virtual host.
- **Virtual Environment:** The type of the virtual environment: **VMware** or **Hyper-V**. This property only appears if the selected Domain Controller runs on a virtual host.
- **Host Info Provider:** Indicates the host metrics collected by the Windows agent or the Active Directory agent.

Click **Next**.

- 3 On the **Assign and Validate Credentials** page, review the available credentials, and edit them, as necessary.
 - To create a new credential, click **Add host(s) to a new credential**.
 - In the **Create New Credential and Assign** dialog box, create a credential that you want to use to access the monitored resource. Type a new credential name, domain, user name, password, and lockbox, and click **Submit**.
 - To select an existing credential, click **Add host(s) to an existing credential**.
 - In the **Select Existing Credential** dialog box, select an existing credential, and click **Submit**.

Click **Next**.

- 4 On the **Summary** page, review the newly updated configuration settings, then click **Finish**.
The **Agent Edit** wizard closes. The agent properties are now updated.

Editing CA agent properties

The **Agent Edit** wizard guides you through the process of editing CA agent properties.

To edit CA agent properties:

- 1 In the *Agent Management > Certificate Authority* view, in the row containing the agent whose properties you want to edit, click the **Edit** column.
- 2 In the **Agent Edit** wizard, on the **Configure CA Agent Properties** page, review the Certificate Authority agent properties, and edit them, as necessary.

- **Host Name:** Type the fully qualified name of a Certificate Authority server.
- **Communication Protocol:** Selects to run the WMI query through DCOM or WinRM.
- **WinRM Port:** The WinRM port number on the monitored Host. This property only appears if the **Communication Protocol** is set to **WinRM through HTTP** or **WinRM through HTTPS**.

i NOTE:

1. When setting **Communication Protocol** as **WinRM through HTTPS**, import the root certificate of the monitoring domain into FglAM keystore.
 2. Ensure that the Subject Alternative Name of the certificate used by LDAP service includes both server FQDN and Domain name.
- For detailed information on how to import certificate into FglAM keystore, refer to [Managing certificates for FglAM](#) on page 42.

Click **Next**.

- 3 On the **Assign and Validate Credentials** page, review the available credentials, and edit them, as necessary.
 - To create a new credential, click **Add host(s) to a new credential**.
 - In the **Create New Credential** dialog box, create a credential that you want to use to access the monitored resource. Type a new credential name, domain, user name, password, and lockbox, and click **Submit**.
 - To select an existing credential, click **Add host(s) to an existing credential**.
 - In the **Assign Credential** dialog box, select an existing credential, and click **Assign**.

Click **Next**.

- 4 On the **CA Summary** page, review the configuration settings chosen for the new agent, and its prerequisite diagnostics, including:
 - **Host Name:** The name of the selected Certificate Authority agent instance.
 - **Communication Protocol:** The communication protocol selected to run the WMI query.
 - **WinRM Port:** The WinRM port number on the monitored Host. This property only appears if the **Communication Protocol** is set to **WinRM through HTTP** or **WinRM through HTTPS**.
 - **Agent Manager:** The name of the selected Foglight Agent Manager Host to be used for the new Certificate Authority agent instances.

Click **Finish**.

The **Agent Edit** wizard closes. The Certificate Authority agent is updated automatically in the Agent Management view, on the *Administration > Certificate Authority* tab.

Inspect agent prerequisites

If any monitoring agents are unable to collect data or connect to the monitored Domain Controllers, you can inspect the underlying cause using the **Prerequisites Diagnostic** button on the Agent Management toolbar.

To examine agent prerequisites:

- 1 In the Agent Management view, select the row containing the agent whose prerequisites you want to examine, and click **Prerequisites Diagnostic** on the toolbar.
- 2 Review the results in the **Prerequisites Diagnostic** dialog box.

- **Agent Name:** The name of the selected Active Directory agent instance.
- **Monitored Host:** The name of the host on which the monitored Domain Controller is running.
- **Diagnostic Result:**
 - **Success:** The agent instance can connect to the monitored Domain Controller and collect data.
 - **Error:** The agent instance cannot connect to the monitored Domain Controller and collect data. Click this link to find out what causes this error. Carefully review the information in the popup that appears in order address the problem.

Managing certificates

Syntax Conventions

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

- Generic examples follow the UNIX path structure that uses forward slashes '/' to separate directories.
- Platform-specific examples follow standard platform conventions. For example, UNIX-specific examples use forward slashes '/' as directory delimiters, while Windows examples use backslashes '\'.
- `<foglight_home>` is a placeholder that represents the path to the Foglight Management Server installation.
- `<foglight_agent_mgr_home>` is a placeholder that represents the path to the Foglight Agent Manager installation. This can be the location of the Foglight Agent Manager installation on a monitored host, or the home directory of the Foglight Agent Manager that comes embedded with the Foglight Management Server. For example:

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

`C:\Quest\Foglight_Agent_Manager`

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

`C:\Quest\Foglight\fglam`

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

Managing certificates for FglAM

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

Prerequisite

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

Add a certificate

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

- Validate the certificate and ensure the following:
 - It is not expired.
 - It is an X.509 format.
 - FglAM requires the Base64 format. To verify if the certificate file is encoded with Base64, open the certificate with a notepad and the certificate should be similar to the following example:


```
-----BEGIN CERTIFICATE-----
```

```
XXXXXXXXXX=
-----END CERTIFICATE-----
```

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

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

List installed certificates

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

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

Refer to the example output below:

```
List of installed certificates:

Alias                  Certificate Info
-----
user alias 1          XXXX
```

Delete a certificate

Remove a certificate referred to by an alias.

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

A full example for managing certificate for FglAM

- Add an example certificate into FglAM certificate store

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

...

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

- List the example certificate in the FglAM certificate store

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

...

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

- Delete the example certificate from the FglAM certificate store

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

...

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

Managing certificates for FMS

Use the keytool utility shipped with Foglight to create, import, or export certificates. This utility can be found at: `<foglight_home>\jre\bin\keytool`.

There are two FMS running modes:

- None-FIPS (Federal Information Processing Standards) mode
- FIPS-compliant mode

Managing certificates for FMS in non-FIPS mode

The KeyStore Foglight used under non-FIPS mode is located at: `<foglight_home>/jre/lib/security/cacerts` (default password: `changeit`)

Add a certificate

Use the keytool command in FMS JRE located in `<foglight>/jre/bin`

```
keytool -import -trustcacerts -alias "<alias>" -file "<certificate path>" -keystore  
<foglight_home>/jre/lib/security/cacerts -storepass changeit
```

- Validate the certificate and ensure the following:
 - It is not expired.
 - It is an X.509 format.
- Change the following before executing the command:
 - `<alias>`: The alias is required and is used in the list and delete operations to refer to the certificate. It can be anything.
 - `<foglight_home>`: The folder path where the Foglight is installed.
 - `<certificate path>`: Your custom certificate path.

List installed certificates

```
keytool -list -keystore <foglight_home>/jre/lib/security/cacerts -storepass changeit
```

Delete a certificate

Remove a certificate referred to by an `alias`.

```
keytool -delete -alias <alias> -keystore <foglight_home>/jre/lib/security/cacerts -  
storepass changeit
```

A full example for managing certificate for FMS in non-FIPS mode

Add example certificate into FMS Certificate Store in non-FIPS mode

```
C:\Quest\Foglight\jre\bin> .\keytool.exe -import -trustcacerts -alias fvegaca -  
file "C:\caca.cer" -keystore C:\Quest\Foglight\jre\lib\security\cacerts -  
storepass changeit  
  
Owner: CN=CA, DC=ca, DC=local  
Issuer: CN=CA, DC=ca, DC=local  
Serial number: xxxxxxxxxxxx  
  
Valid from: Mon Jun 15 10:56:05 CST 2015 until: Mon Sep 23 14:58:03 CST 2047  
Certificate fingerprints:  
    MD5:  xxxx  
    SHA1:  xxxx
```

```

SHA256: xxxx

.....

Trust this certificate? [no]: yes

Certificate was added to keystore

```

Managing certificates for FMS in FIPS-compliant mode

The KeyStore Foglight used in FIPS-compliant mode is located at:
 <foglight_home>/config/security/trust.fips.keystore (default password: nitrogen)

Add a certificate in FIPS-compliant mode

Use the keytool command in FMS JRE located in <foglight>/jre/bin.

```

keytool -import -trustcacerts -alias "<alias>" -file "<certificate path>" -keystore
"<Foglight_home>/config/security/trust.fips.keystore" -deststoretype BCFKS -
provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"<Foglight_home>/server/core/bc-fips.jar" -storepass nitrogen

```

- Validate the certificate and ensure the following:
 - It is not expired.
 - It is an X.509 format.
- Change the following before executing the command
 - <alias>: The alias is required and is used in the list and delete operations to refer to the certificate. It can be anything.
 - <Foglight_home>: The folder path where Foglight is installed.
 - <certificate path>: Your custom certificate path.

List installed certificates

```

keytool -list -keystore "<Foglight_home>/config/security/trust.fips.keystore" -
deststoretype BCFKS -provider
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"<Foglight_home>/server/core/bc-fips.jar" -storepass nitrogen

```

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

Refer to the example output below:

```

Keystore type: BCFKS

Keystore provider: BCFIPS

Your keystore contains 151 entries

camerfirmachambersignca [jdk], Dec 18, 2019, trustedCertEntry,
Certificate fingerprint (SHA1):
4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C

entrust2048ca [jdk], Dec 18, 2019, trustedCertEntry

...

```

Delete a certificate

Remove a certificate referred to by an alias.

```

keytool -delete -alias <alias> -keystore
"<Foglight_home>/config/security/trust.fips.keystore" -deststoretype BCFKS -
provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"<Foglight_home>/server/core/bc-fips.jar" -storepass nitrogen

```

A full example for managing certificate for FMS in FIPS-compliant mode

Add example certificate into FMS certificate store in FIPS-compliant mode

```
C:\Quest\Foglight\jre\bin>keytool -import -trustcacerts -alias "Evolve-Test" -file
"D:/Evolve-test.crt" -keystore
"C:/Quest/Foglight/config/security/trust.fips.keystore" -deststoretype BCFKS -
provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"C:/Quest/Foglight/server/core/bc-fips.jar" -storepass nitrogen

Owner: CN=CA, DC=ca, DC=local
Issuer: CN=CA, DC=ca, DC=local
Serial number: xxxx
Valid from: Sun Jan 06 23:07:06 CST 2019 until: Wed Apr 06 23:07:06 CST 2022
Certificate fingerprints:
...

Extensions:
...

Trust this certificate? [no]: yes
Certificate was added to keystore
```

Active Directory agent properties

The primary properties for an Active Directory® agent instance are required to connect to the target server from which data is to be collected. These properties are either specified when the agent instance is configured or they have a pre-defined default value.

To display an agent's properties page, use one of the following methods:

- From the navigation panel, navigate to **Dashboards > Administration > Agents > Agent Properties**. On the Agent Properties dashboard, select an agent. The Properties panel is displayed, showing the current properties for the selected agent instance.
- From the navigation panel, navigate to **Dashboards > Administration > Agents > Agent Status**. On the Agent Status dashboard, select an agent from the list and click **Edit > Edit Properties**. The Agent Status dashboard refreshes, showing the current properties for the selected agent instance.

Figure 18. Agent properties page

Agent Status > Edit Properties

Host: dlu1.prod.quest.corp, Type: ActiveDirectory

Configuration:

- Host Name: dc6.domain6.local
- Host collector: VMWare (must be installed)
- Communication Protocol: DCOM
- WinRM Port: 5985
- Enable SSL For LDAP: ☐ True ☒ False
- LDAP Authentication Scheme: Kerberos
- Activate adobjects Collector: ☒ True ☐ False
- Network Connection TimeOut: 51000

Monitor:

- Monitored Services: defaultServices

Unavailable WMI Classes:

- WMI Classes: unavailableClasses

Data Collection Scheduler:

- Collector Config: defaultSchedule

Buttons: Cancel, Save

For more information on using the Agent Status dashboard to edit agent properties, see the *Foglight Administration and Configuration Help*.

The following tables describe the properties that can be modified for either an individual or all Active Directory agent instances, by clicking **Modify the private properties for this agent** or **Modify the properties of all ActiveDirectory agents** links, respectively.

NOTE: It is recommended to configure the agent properties that are to be applied globally to the majority of the Active Directory agent instances, then modify the private properties of those individual agents, as required.

For additional information, see these topics:

- [Configuration](#)
- [Monitor](#)
- [Unavailable WMI Classes](#)
- [Data Collection Scheduler](#)

Configuration

Use the properties in the Configuration panel to specify the target server from which data is to be collected, to define what cartridge is to be used to collect the host metrics, and specify whether the target server is a virtual machine.

NOTE: The properties defined here apply to either a single Active Directory® agent or all agents with the type of ActiveDirectory, based on the option selected at the top of the agent properties page.

Table 10. Configuration panel

Property	Default	Description
Host Name	N/A	The fully qualified domain name (<i>myServer.myDomain.com</i>) of the target server from which data is to be collected.
Host Collector		<p>The host metrics (CPU, Memory, Network, Storage) displayed in Foglight for Active Directory can be collected by the Foglight for Active Directory, Foglight for Hyper-V, Foglight for VMware, or Foglight for Infrastructure cartridge.</p> <p>NOTE: If you have Foglight for Hyper-V or Foglight for VMWare installed, it is best to select the corresponding option and use the metrics collected by that cartridge.</p> <p>NOTE: If you are collecting host metrics on a virtual machine using Foglight for Active Directory, performance counters may be subject to known inconsistencies because in-guest performance counters can be skewed by virtualization. To collect the most accurate host metrics on a virtual machine, use Foglight for VMWare or Foglight for Hyper-V to collect these metrics.</p> <p>Select the host collector to be used to collect host metrics:</p> <ul style="list-style-type: none"> • AD (included) - if selected, all host collections are collected based on the interval set in the collection schedule. • Hyper-V (must be installed) - if selected, the logical disk space metrics are collected based on the interval set in the collection schedule; all other host metrics are collected based on the settings in the Foglight for Hyper-V cartridge. The “Memory In Use” is not available and will be blank in this configuration. • VMWare (must be installed) - if selected, the host collections are skipped regardless of the value in the collection schedule. That is, all host collections are collected based on the settings in the Foglight for VMWare cartridge. • Infrastructure (must be installed) - if selected, the host collections are skipped regardless of the value in the collection schedule. That is, all host collections are collected based on the settings in the Foglight for Infrastructure cartridge.
Communication Protocol	WinRM Through HTTPS	Selects to run the WMI query through DCOM , WinRM Through HTTP , or WinRM Through HTTPS .
WinRM Port	5986	Determines the WinRM port number in the monitored server.
Enable SSL For LDAP	False	Enables/ disables security LDAP connection.
LDAP Authentication Scheme	Basic	Supports both <i>Basic</i> and <i>Kerberos</i> authentication schemes, when connected to LDAP server.

Table 10. Configuration panel

Property	Default	Description
Activate adobjects Collector	True	Turns on/ off the <i>adobjects</i> (user count, groups count, computer count) collection. In one domain, it only needs one agent to collect such information.
Network Connection TimeOut	51,000	Specifies how long (milliseconds) the system waits for a response from the remote server before it times out. That is, this is the time in milliseconds that a data collection query will run before it is presumed to have failed and the network connection is terminated.

Monitor

The selection made in the *Monitor* panel of the properties page defines the services that are to be monitored by the selected agent(s).

NOTE: The setting in this section is global and applies to all agents with the type of ActiveDirectory.

The services monitored by default are:

- DFSR
- NtFrs
- W32Time
- Netlogon
- SamSs
- kdc
- Dnscache
- IsmServ
- RpcSs
- DNS
- Winmgmt
- LanmanServer
- LanmanWorkstation

Unavailable WMI Classes

The *Unavailable WMI Classes* panel allows users to disable invalid WMI queries, caused by WMI classes unavailable for an environment issue.

Data Collection Scheduler

The selection made in the *Data Collection Scheduler* panel defines the data collection schedule to be used.

NOTE: The settings in this section are global and apply to all agents with the type of ActiveDirectory.

The following table lists the collectors being used by the cartridge and the default collection interval for each (as defined in the defaultSchedule).

The collections marked with an asterisk indicate collections with corresponding sections on the Active Directory Metrics Management dashboard. When using the defaultSchedule, you can use either this setting on the agent properties page or the Metrics Management dashboard to modify these connection intervals. For those collectors not marked with an asterisk or if you are using a user-defined data collection schedule, you must use this setting to manage the data collection intervals. For more information on the Active Directory Metrics Management dashboard, see [Managing Active Directory metrics](#).

Table 11. Default collection interval

Collector Name	Default Collection Interval
domain	1 day
adobjects	1 day
time	30 minutes
replication*	4 minutes
site	1 hour
database	4 minutes
role	15 minutes
dns*	6 minutes
frs*	5 minutes
dfs*	6 minutes
directoryService*	4 minutes
daily	1 day
hostDetail	5 minutes
dotNetFramework	7 minutes
ping	2 minutes

Reporting on your Active Directory enterprise

Foglight for Active Directory comes with a set of pre-defined reports that can be run from the Reports dashboard. Using this dashboard, operators can run reports, build custom reports, and view generated reports. Advanced Operators can also schedule and manage reports.

To access the Reports dashboard, from the Foglight navigation pane, select **Dashboards > Reports**. From the Reports dashboard, click the links provided as described below:

- Click **Build a Custom Report** to choose the building blocks for your custom report using the Create a Report wizard.
- Click **Run a Report** to quickly generate a one-time report based on a template, using the Run a Report wizard.
- Click **Manage Reports** to access the Manage Reports dashboard, where you can download, delete and view details about generated reports.

NOTE: You can also create a new report using the General tab on the Action panel to the right of any dashboard. Select the Create report option under the Other Actions list to launch the Create Report wizard to define the components to be used to build a new report.

For more information on using the Foglight reporting features, see the *Foglight User Guide* or online help.

Foglight for Active Directory reports

Several different report templates are available with Foglight for Active Directory, and together they provide a detailed analysis of the performance and health of your Active Directory® environment over time.

Each report template uses report parameters to define the content of the report. Use a template's default report parameters to quickly generate or schedule a report or optionally change the report parameters to customize the report to better meet your requirements.

The following table contains an alphabetical list of Foglight for Active Directory reports. It also provides a brief description of the report and the report parameters used to define the content. Report parameters marked with an asterisk (*) are required and you must specify this parameter before the report can be generated.

NOTE: If you are using the Templates by Module tab on the Generate Report dialog, click the expansion box to the left of the Active Directory entry to view the Active Directory reports.

Table 12. Foglight for Active Directory report templates

Report	Description	Report Parameters: Default
Active Directory Alarms	Displays the outstanding Active Directory alarms.	<ul style="list-style-type: none"> • Time Range: Last 4 hours
Diagnostic Test - History	Displays the result for all runs of an Active Directory Diagnostic Test.	<ul style="list-style-type: none"> • Time Range: Last 4 hours • * Test • Target Server Filter: Null

Table 12. Foglight for Active Directory report templates

Report	Description	Report Parameters: Default
Diagnostic Test Result Detail Report	Displays the Diagnostic Test result details.	<ul style="list-style-type: none"> • *Test • *Target Server • *Test Run
Diagnostic Test Result Report	Displays the Diagnostic Test results.	<ul style="list-style-type: none"> • Time Range: Last 4 hours • *Test • Target Server Filter
Domain Controller FAQTs	Shows all FAQTs for the selected DCs.	<ul style="list-style-type: none"> • Time Range: Last 4 hours • * Domain Controllers
Domain Controller FAQTS for Domain	Shows domain controller FAQTs for the selected domain.	<ul style="list-style-type: none"> • Time Range: Last 4 hours • * Domain
Domain Controller FAQTS for Forest	Shows domain controller FAQTs for the selected forest.	<ul style="list-style-type: none"> • Time Range: Last 4 hours • * Forest
Domain Controller FAQTS for Site	Shows domain controller FAQTs for the selected site.	<ul style="list-style-type: none"> • Time Range: Last 4 hours • * Site
Domain Controller Inventory for Domain	Shows the DCs in the selected domain.	<ul style="list-style-type: none"> • Time Range: Last 4 hours • * Domain
Domain Controller Utilization - Detail	<p>Shows the top and bottom DCs based on CPU Used Hz, CPU percent privileged time, memory consumed, disk utilization, disk transfer rate and network transfer rate for the specified time range. It also displays additional details.</p> <p>NOTE: The CPU Used Hz metric can be used to compare relative CPU utilization across different systems.</p>	<ul style="list-style-type: none"> • Time Range: Last 4 hours • DC Count: 25
Domain Controller Utilization - Summary	<p>Shows the top and bottom five DCs based on CPU Used Hz, CPU percent privileged time, memory consumed, disk utilization, disk transfer rate and network transfer rate for the specified time range.</p> <p>NOTE: The CPU Used Hz metric can be used to compare relative CPU utilization across different systems.</p>	<ul style="list-style-type: none"> • Time Range: Last 4 hours
Domain Controllers Available CPU and Memory - Detail	Shows the top and bottom DCs based on available CPU and memory.	<ul style="list-style-type: none"> • Time Range: Last 4 hours • DC Count: 25
Domain Controllers Available CPU and Memory - Summary	Shows the top and bottom five DCs based on available CPU and memory.	<ul style="list-style-type: none"> • Time Range: Last 4 hours
Domain Controllers Storage	Shows the capacity and usage of logical and physical disks on the selected DCs.	<ul style="list-style-type: none"> • Time Range: Last 4 hours
Domains FAQTS	Shows the domain FAQTs for the selected domains.	<ul style="list-style-type: none"> • Time Range: Last 4 hours • * Domains

Table 12. Foglight for Active Directory report templates

Report	Description	Report Parameters: Default
Forest Domain Inventory	Shows the DCs in each domain in the selected forest.	<ul style="list-style-type: none"> Time Range: Last 4 hours * Forest
Forest FAQTS	Shows the forest FAQts for the selected forests.	<ul style="list-style-type: none"> Time Range: Last 4 hours * Forest
Logical Disks With X% Or Less Free Storage - Detail	Displays the DC count, logical disk count, total disk space available, and total disk space used for all DCs with x% or less free storage. It also displays additional details.	<ul style="list-style-type: none"> Time Range: Last 4 hours * Percent
Logical Disks With X% Or Less Free Storage - Summary	Displays the DC count, logical disk count, total disk space available, and total disk space used for all DCs with x% or less free storage.	<ul style="list-style-type: none"> Time Range: Last 4 hours * Percent
Logical Disks With X% Or More Free Storage - Detail	Displays the DC count, logical disk count, total disk space available, and total disk space used for all DCs with x% or more free storage. It also displays additional details.	<ul style="list-style-type: none"> Time Range: Last 4 hours * Percent
Logical Disks With X% Or More Free Storage - Summary	Displays the DC count, logical disk count, total disk space available, and total disk space used for all DCs with x% or more free storage.	<ul style="list-style-type: none"> Time Range: Last 4 hours * Percent
Site FAQTS	Shows the site FAQts for the selected sites.	<ul style="list-style-type: none"> Time Range: Last 4 hours * Site

Foglight for Active Directory views

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

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 can be added to dashboards or can be accessed by drilling down from a dashboard. They receive and display data directly from the Foglight 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.

This section provides a description of the lower-level views on Foglight for Active Directory dashboards. The beginning of the section explains which views are available to find specific information for each of the Active Directory® objects:

- [Forest views](#)
- [Domain views](#)
- [Site views](#)
- [Domain Controller views](#)

The latter part of the section provides a detailed description of the information and metrics displayed in embedded views:

- [Description of embedded views](#)

Forest views

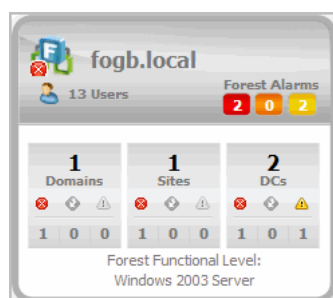
A forest is the top-level object within the Active Directory® infrastructure and consists of a group of Active Directory domains. The following views are available to monitor the health of your Active Directory forests:

- [Forests Environment Summary \(All Forests\) view](#)
- [Forest Environment Summary view](#)
- [Forests Explorer Summary \(All Forests\) view](#)
- [Forest Explorer Summary view](#)

Forests Environment Summary (All Forests) view

The Forests Environment Summary (All Forests) view displays a forest tile for each forest in your Active Directory® environment that provides summary data about the different object types (domains, sites and DCs) within each forest and the number of objects in each of the alarm states (fatal, critical and warning).

Figure 19. Forests Environment Summary (All Forests) view



A forest tile displays the following information:

- name of the forest
- number of users in the forest
- number of alarms in each state in the forest
- number of domains in the forest and number of domains in each alarm state
- number of sites in the forest and number of sites in each alarm state
- number of DCs in the forest and number of DCs in each alarm state
- Forest Functional Level

How to get here

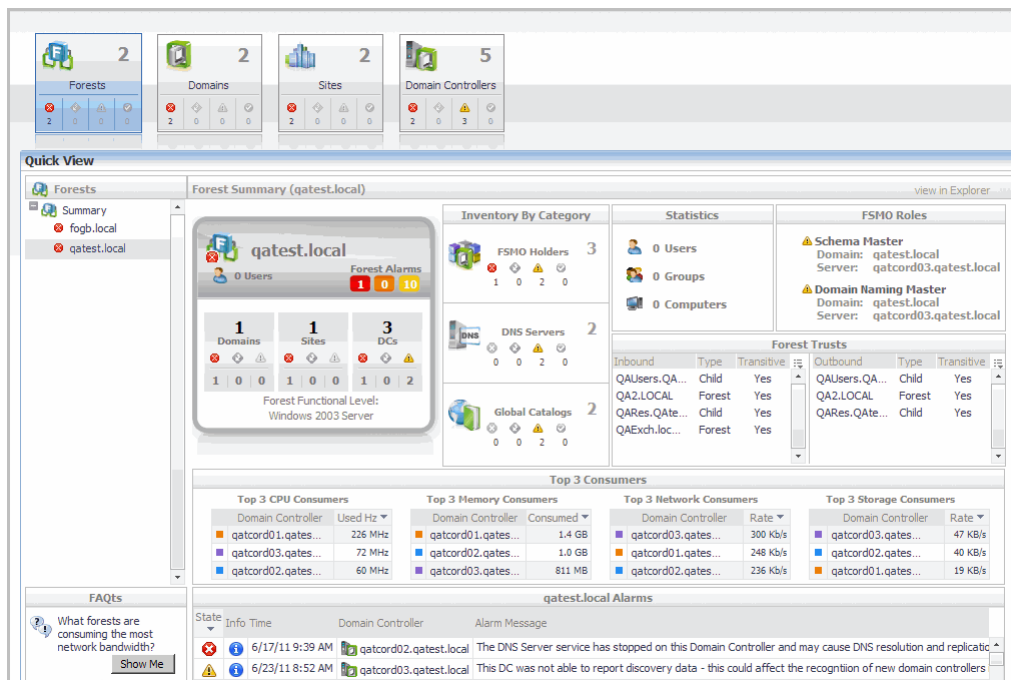
- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Environment**.
- 2 From the Monitoring tab, select the **Forests** tile.
- 3 From the Object Tree view, select **Summary**.

The Forests Environment Summary (All Forests) view appears in the Object Summary view of the Quick View on the Active Directory Environment dashboard.

Forest Environment Summary view

The Forest Environment Summary view displays a forest tile for the selected forest, showing the object types within this forest and the alarm states for each. In addition to the forest tile, this display provides more detailed information about the accounts, roles, and trusts in the selected forest. It also shows the top DCs in the forest that are consuming the most computer resources.

Figure 20. Forest Environment Summary view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Environment**.
- 2 From the Monitoring tab, select the **Forests** tile.
- 3 From the Object Tree view, select an individual **Forest object**.

The Forest Environment Summary view appears in the Object Summary view of the Quick View on the Active Directory Environment dashboard.

NOTE: You can also click a forest tile in the Forests Environment Summary (All Forests) view to display this view.

Embedded views

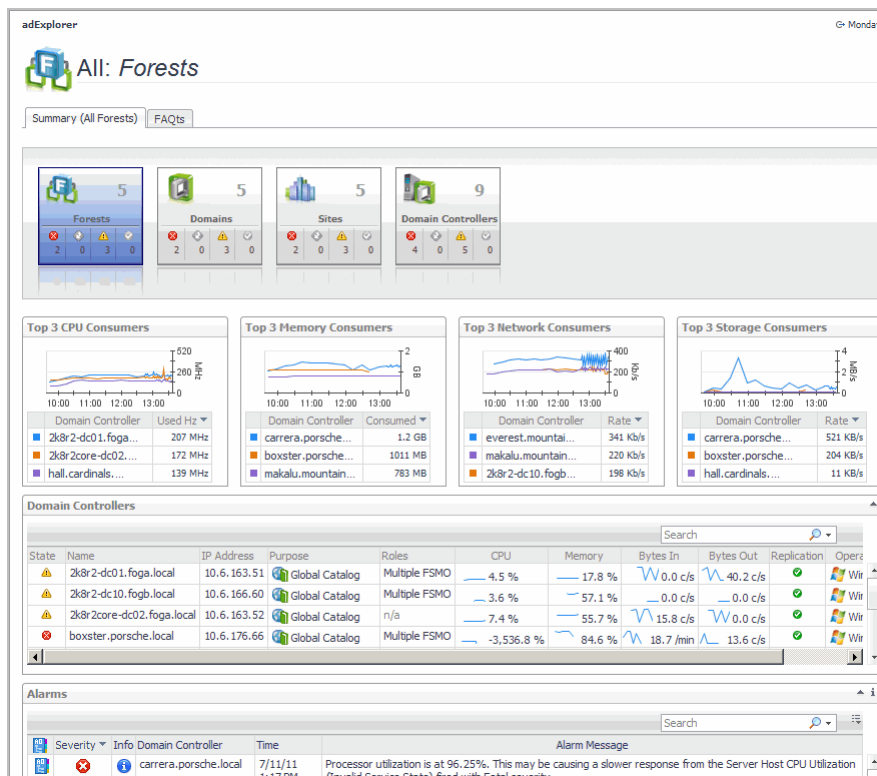
In addition to the forest tile, the following embedded views are displayed in the Forest Summary:

- [Inventory By Category view](#)
- [Statistics view](#)
- [FSMO Roles view \(Forest\)](#)
- [Trusts view](#)
- [Top 3 Consumers view](#)

Forests Explorer Summary (All Forests) view

The Forests Explorer Summary (All Forests) view displays detailed resource metrics and information for the DCs in all of the monitored forests in your Active Directory® environment.

Figure 21. Forests Explorer Summary (All Forests) view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 From the Active Directory Enterprise view (under Dashboards in the navigation panel), select the **Forests object container**.

The Forests Explorer Summary (All Forests) view appears in the Primary view on the Active Directory Explorer dashboard.

NOTE: You can also click the view in Explorer link on the Forests Environment Summary (All Forests) view.

Embedded views

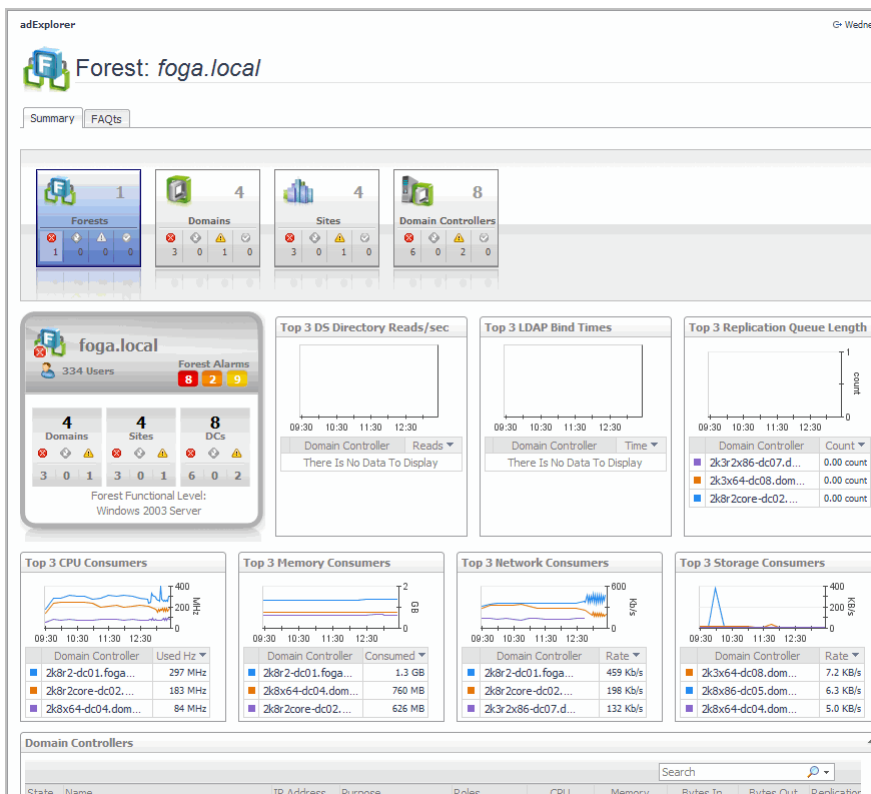
In addition to the current forest alarms, this view is made up of the following embedded views:

- [Top 3 CPU Consumers view](#)
- [Top 3 Memory Consumers view](#)
- [Top 3 Network Consumers view](#)
- [Top 3 Storage Consumers view](#)
- [Domain Controllers view](#)

Forest Explorer Summary view

The Forest Explorer Summary view displays detailed resource metrics and information about the DCs in the selected Active Directory® forest.

Figure 22. Forest Explorer Summary view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 Use one of the following methods to display this view:
 - From the Active Directory Enterprise view (under Dashboards in the navigation panel), select an individual **Forest object**.
 - From the Forests tile (at the top of the Summary view), click the **Forests** icon, title or count. On the Forests Inventory dialog, select an individual **Forest object**.

The Forest Explorer Summary view appears in the Primary view on the Active Directory Explorer dashboard.

NOTE: You can also click the view in Explorer link on the Forest Environment Summary view for the selected forest.

Embedded views

In addition to the forest tile and current alarms, this view is made up of the following embedded views:

- [Top 3 DS Directory Reads/sec view](#)
- [Top 3 LDAP Bind Times view](#)
- [Top 3 Replication Queue Length view](#)
- [Top 3 CPU Consumers view](#)
- [Top 3 Memory Consumers view](#)
- [Top 3 Network Consumers view](#)
- [Top 3 Storage Consumers view](#)

- [Domain Controllers view](#)

Domain views

A Domain is a partition of the Active Directory® forest used to implement directory security and to manage resources.

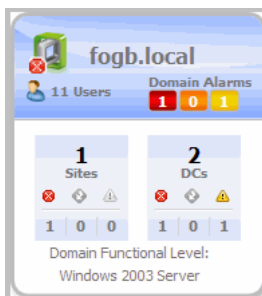
The following views are available to monitor the health of your Active Directory domains:

- [Domains Environment Summary \(All Domains\) view](#)
- [Domain Environment Summary view](#)
- [Domains Explorer Summary \(All Domains\) view](#)
- [Domain Explorer Summary view](#)

Domains Environment Summary (All Domains) view

The Domains Environment Summary (All Domains) view displays a domain tile for each domain in your Active Directory® environment. These domain tiles display summary data about the different sites and DCs that reside in each domain, as well as the number of objects in each of the alarm states (fatal, critical and warning).

Figure 23. Domains Environment Summary (All Domains) view



A domain tile displays the following information:

- name of the domain
- number of users in the domain
- number of domain alarms in each state
- number of sites in the domain and number of sites in each alarm state
- number of DCs in the domain and number of DCs in each alarm state
- Domain Functional Level

How to get here

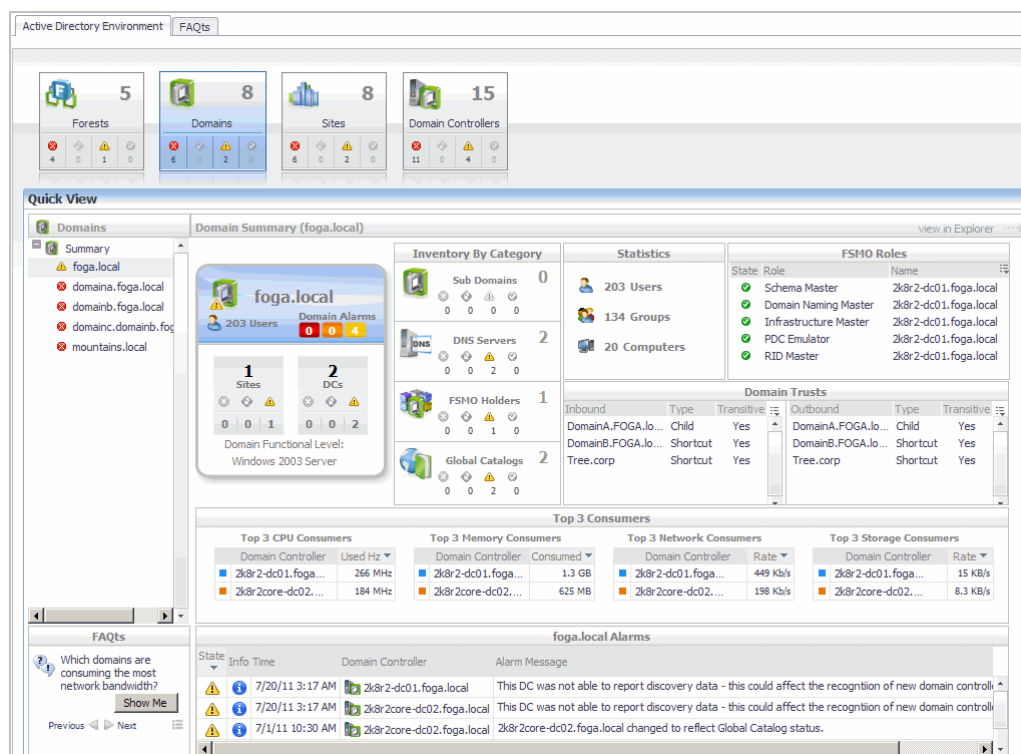
- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Environment**.
- 2 From the Monitoring tab, select the **Domains** tile.
- 3 From the Object Tree view, select **Summary**.

The Domains Environment Summary (All Domains) view appears in the Object Summary view of the Quick View on the Active Directory Environment dashboard.

Domain Environment Summary view

The Domain Environment Summary view displays a domain tile for the selected domain, showing data about the object types within that domain and the number of objects in each of the alarm states. In addition to the domain tile, this view displays more detailed information about the accounts, roles, and trusts in the selected domain. It also shows the top DCs in the domain that are consuming the most computer resources.

Figure 24. Domain Environment Summary view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Environment**.
- 2 From the Monitoring tab, select the **Domains** tile.
- 3 From the Object Tree view, select an individual **Domain object**.

The Domain Environment Summary view appears in the Object Summary view of the Quick View on the Active Directory Environment dashboard.

NOTE: You can also click a domain tile in the Domains Environment Summary (All Domains) view to display this view.

Embedded views

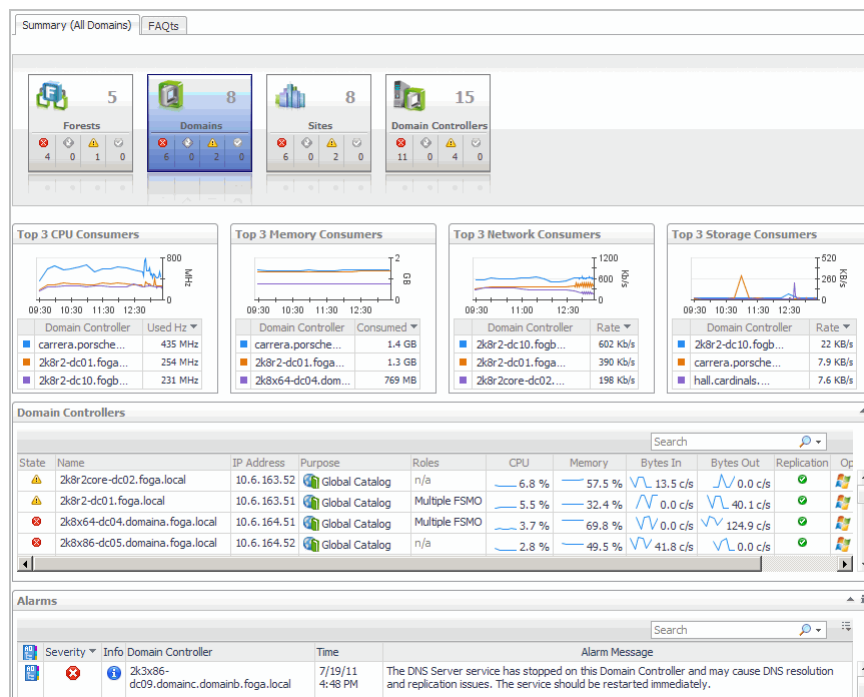
In addition to the domain tile, the following embedded views are displayed in the Domain Summary:

- [Inventory By Category view](#)
- [Statistics view](#)
- [FSMO Roles view \(Domain\)](#)
- [Trusts view](#)
- [Top 3 Consumers view](#)

Domains Explorer Summary (All Domains) view

The Domains Explorer Summary (All Domains) view displays detailed resource metrics and information for the DCs in all of the monitored domains in your Active Directory® environment.

Figure 25. Domains Explorer Summary (All Domains) view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 From the Active Directory Enterprise view (under Dashboards in the navigation panel), select the **Domain object container**.

The Domains Explorer Summary (All Domains) view appears in the Primary view on the Active Directory Explorer dashboard.

NOTE: You can also click the view in Explorer link on the Domains Environment Summary (All Domains) view.

Embedded views

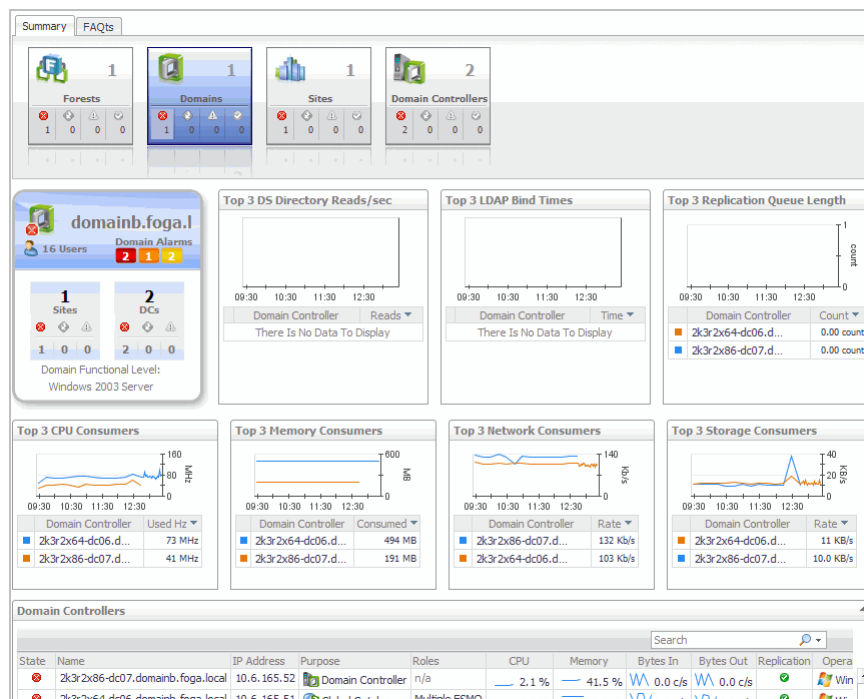
In addition to the current domain alarms, this view is made up of the following embedded views:

- [Top 3 CPU Consumers view](#)
- [Top 3 Memory Consumers view](#)
- [Top 3 Network Consumers view](#)
- [Top 3 Storage Consumers view](#)
- [Domain Controllers view](#)

Domain Explorer Summary view

The Domain Explorer Summary view displays detailed resource metrics and information for the DCs in the selected domain.

Figure 26. Domain Explorer Summary view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 Use one of the following methods to display this view:
 - From the Active Directory Enterprise view (under Dashboards in the navigation panel), select an individual **Domain object**.
 - From the Domains tile (at the top of the Summary view), select the **Domains** icon, title or count. On the Domains Inventory dialog, select an individual **Domain object**.

The Domain Explorer Summary view appears in the Primary view on the Active Directory Explorer dashboard.

NOTE: You can also click the view in Explorer link on the Domain Environment Summary view for the selected domain.

Embedded views

In addition to the domain tile and current alarms, this view is made up of the following embedded views:

- [Top 3 DS Directory Reads/sec view](#)
- [Top 3 LDAP Bind Times view](#)
- [Top 3 Replication Queue Length view](#)
- [Top 3 CPU Consumers view](#)
- [Top 3 Memory Consumers view](#)
- [Top 3 Network Consumers view](#)

- [Top 3 Storage Consumers view](#)
- [Domain Controllers view](#)

Site views

A Site represents a logical grouping of computers within Active Directory® that have reliable connectivity. Active Directory uses the site layout to create the best replication topology for the DCs in the forest. Site topology is not related to the domain hierarchy. That is, a domain can appear in many sites, and a site can contain many domains.

When you know the location of a directory problem, the Site views provide a quick way to get the metrics about the site and DCs in that site.

NOTE: If you create a new site in a monitored domain, to start collecting data about that site, you must restart the monitoring Active Directory agent. If a domain controller is not located in a newly added or removed from your environment, the change is reflected only after the replication process between the associated domain controllers is finished, and the agent is restarted.

To determine the length of time needed to process replications on individual sites, issue the following command:

```
repadmin /latency <DC_LIST>
```

For more information, visit [http://technet.microsoft.com/en-ca/library/cc811567\(v=ws.10\).aspx](http://technet.microsoft.com/en-ca/library/cc811567(v=ws.10).aspx).

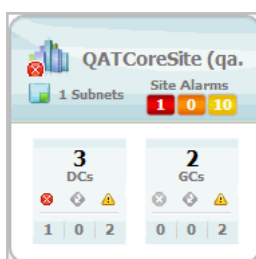
The following views are available to monitor the health of the sites within your Active Directory infrastructure:

- [Sites Environment Summary \(All Sites\) view](#)
- [Site Environment Summary view](#)
- [Sites Explorer Summary \(All Sites\) view](#)
- [Site Explorer Summary view](#)

Sites Environment Summary (All Sites) view

The Sites Environment Summary (All Sites) view displays a site tile for each site in your Active Directory® environment and provides summary data about the DCs and Global Catalog servers (GCs) within each site. It also displays the number of DCs and GCs in each of the alarm states (fatal, critical and warning) for each site.

Figure 27. Sites Environment Summary (All Sites) view



A site tile displays the following information:

- name of the site
- number of subnets in the site
- number of site alarms in each state
- number of DCs in the site and number of DCs in each alarm state

- number of GCs in the site and number of GCs in each alarm state

How to get here

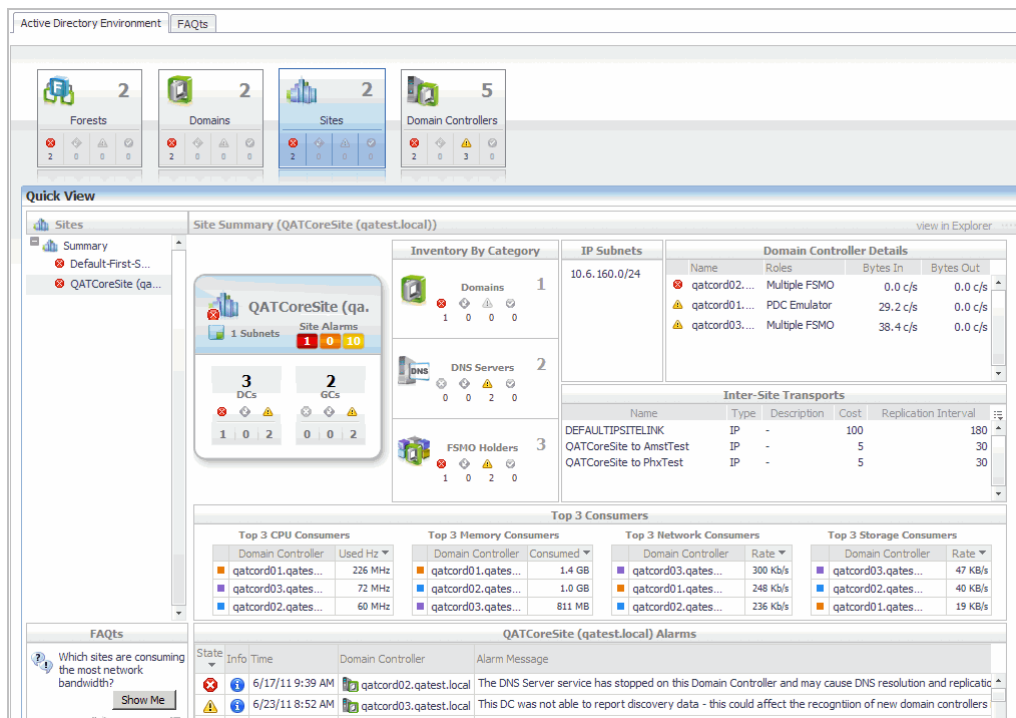
- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Environment**.
- 2 From the Monitoring tab, select the **Sites** tile.
- 3 From the Object Tree view, select **Summary**.

The Sites Environment Summary (All Sites) view appears in the Object Summary view of the Quick View on the Active Directory Environment dashboard.

Site Environment Summary view

The Site Environment Summary view displays a site tile for the selected site, showing data about the object types within that site and the number of objects in each of the alarm states. In addition to the site tile, this view displays details about the DCs, subnets and transports that make up this site.

Figure 28. Site Environment Summary view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Environment**.
- 2 From the Monitoring tab, select the **Sites** tile.
- 3 From the Object Tree view, select an individual **Site object**.

The Site Environment Summary view appears in the Object Summary view of the Quick View on the Active Directory Environment dashboard.

NOTE: You can also click a site tile in the Sites Environment Summary (All Sites) view to display this view.

Embedded views

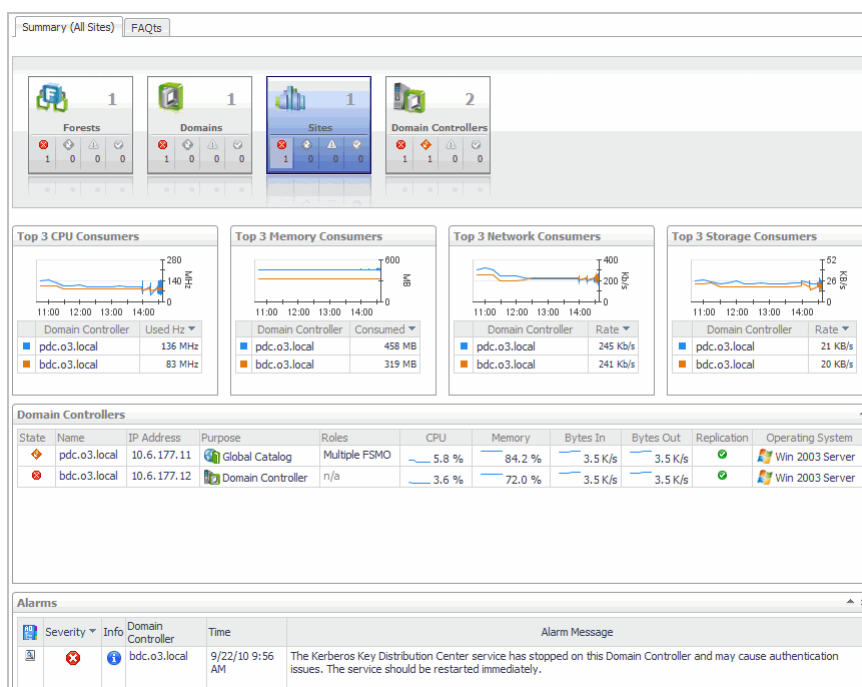
In addition to the site tile and current site alarms, the following embedded views are displayed in the Site Summary:

- [Inventory By Category view](#)
- [IP Subnets view](#)
- [Domain Controller Details view](#)
- [Inter-Site Transports view](#)
- [Top 3 Consumers view](#)

Sites Explorer Summary (All Sites) view

The Sites Explorer Summary (All Sites) view displays detailed resource metrics and information about the DCs in all of the monitored sites in your Active Directory® environment.

Figure 29. Sites Explorer Summary (All Sites) view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 From the Active Directory Enterprise view (under Dashboards in the navigation panel), select the **Sites object container**.

The Sites Explorer Summary (All Sites) view appears in the Primary view on the Active Directory Explorer dashboard.

NOTE: You can also click the view in Explorer link on the Sites Environment Summary (All Sites) view.

Embedded views

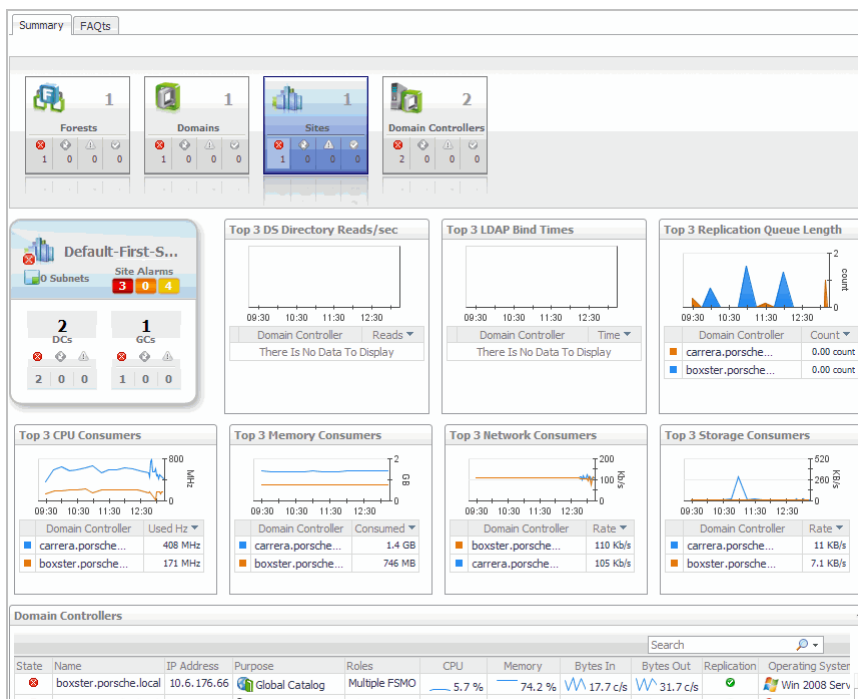
In addition to the current site alarms, this view is made up of the following embedded views:

- [Top 3 CPU Consumers view](#)
- [Top 3 Memory Consumers view](#)
- [Top 3 Network Consumers view](#)
- [Top 3 Storage Consumers view](#)
- [Domain Controllers view](#)

Site Explorer Summary view

The Site Explorer Summary view displays more detailed resource metrics and information about the DCs in the selected site.

Figure 30. Site Explorer Summary view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 Use one of the following methods to display this view:
 - From the Active Directory Enterprise view (under Dashboards in the navigation panel), select an individual **Site object**.
 - From the Sites tile (at the top of the Summary view), select the **Sites** icon, title or count. On the Sites Inventory dialog, select an individual **Site object**.

The Site Explorer Summary view appears in the Primary view on the Active Directory Explorer dashboard.

NOTE: You can also click the view in Explorer link on the Site Environment Summary view for the selected site.

Embedded views

In addition to the site tile and current alarms, this view is made up of the following embedded views:

- [Top 3 DS Directory Reads/sec view](#)
- [Top 3 LDAP Bind Times view](#)
- [Top 3 Replication Queue Length view](#)
- [Top 3 CPU Consumers view](#)
- [Top 3 Memory Consumers view](#)
- [Top 3 Network Consumers view](#)
- [Top 3 Storage Consumers view](#)
- [Domain Controllers view](#)

Domain Controller views

A Domain Controller (DC) is a server that is running a version of the Windows Server® operating system and has Active Directory® (Windows Server 2003) or Active Directory® Domain Services (Windows Server® 2008 R2 and Windows Server 2008) installed. The DC is tasked with managing a replica of an Active Directory domain.

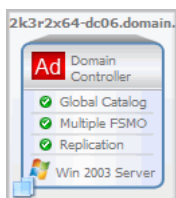
The following views are available to monitor the health of your Active Directory domain controllers:

- [Domain Controllers Environment Summary \(All DCs\) view](#)
- [Domain Controller Environment Summary view](#)
- [Domain Controllers Explorer Summary \(All DCs\) view](#)
- [Domain Controller Explorer Summary view](#)
- [Resource Utilization Details view](#)
- [Domain Controller Database view](#)
- [Domain Controller Directory Services view](#)
- [Domain Controller DFS-R view](#)
- [Domain Controller FRS view](#)
- [Domain Controller Replication view](#)

Domain Controllers Environment Summary (All DCs) view


By default, the Domain Controllers Environment Summary (All DCs) view displays a domain controller tile for each DC in your Active Directory® environment and provides summary data about the different roles performed by each DC. It also includes an alarm indicator for each of these roles.

Figure 31. Domain Controllers Environment Summary (All DCs) view



A domain controller tile displays the following information:

- name of the DC and its current alarm state

- list of roles performed by the DC and their current alarm state
- Windows® operating system running on the server
- the  icon in the lower left corner indicates that the DC is a virtual machine that is being monitored by Foglight for VMWare or Foglight for Hyper-V. In addition, the domain controller tile is outlined in blue when it is a virtual machine that is being monitored by one of these cartridges.

NOTE: If you would prefer to view a list of DCs, instead of tiles for each DC, select **Toggle View**. You can then use the search controls to the right to filter your list of DCs.

How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Environment**.
- 2 From the Monitoring tab, select the **Domain Controllers** tile.
- 3 From the Object Tree view, select **Summary**.

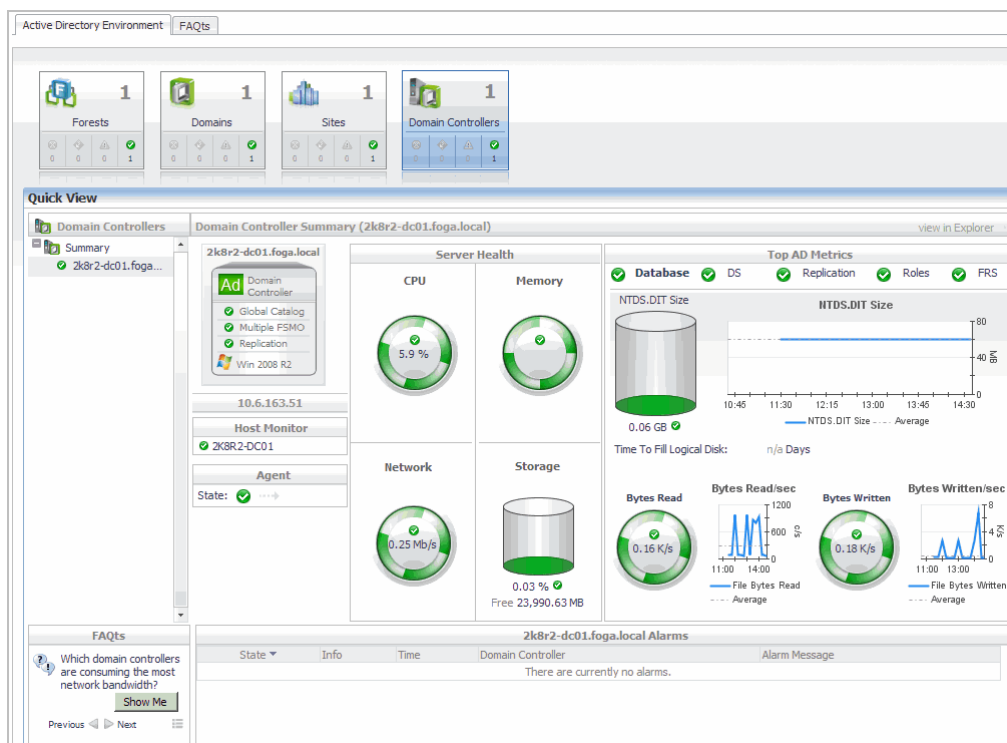
The Domain Controllers Environment Summary (All DCs) view appears in the Object Summary view of the Quick View on the Active Directory Environment dashboard.

Domain Controller Environment Summary view

The Domain Controller Environment Summary view displays a domain controller tile for the selected DC and shows data relevant to that DC, the current alarm state for the DC, and the roles being performed by the DC.

NOTE: If the Server Health metrics are not appearing on this view, check the Host Collector setting on the agent's properties page. The VMWare option is selected by default. If Foglight for Active Directory, Foglight for Hyper-V, or Foglight for Infrastructure is being used to collect the host metrics, this setting must be set to the appropriate option.

Figure 32. Domain Controller Environment Summary view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Environment**.
- 2 From the Monitoring tab, select the **Domain Controllers** tile.
- 3 From the Object Tree view, select an individual **DC object**.

The Domain Controller Environment Summary view appears in the Object Summary view of the Quick View on the Active Directory Environment dashboard.

i | **NOTE:** You can also click a domain controller tile in the Domain Controllers Environment Summary (All DCs) view to display this view.

Embedded views

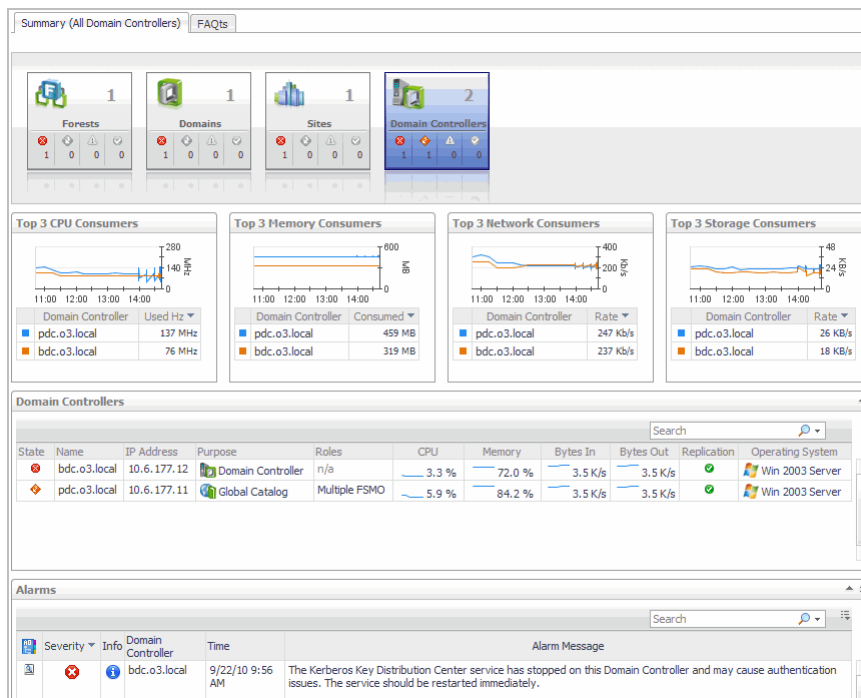
In addition to the domain controller tile, the following embedded views are displayed on the Domain Controller Summary:

- [Host Monitor view](#)
 - i** | **NOTE:** When the host machine is a virtual machine that is being monitored by Foglight for VMWare or Foglight for Hyper-V, this view is replaced with two views: one that displays the name of the virtual machine and one that displays the name of the host server.
- [Agent State view](#)
- [Server Health view](#)
- [Top AD Metrics view](#)

Domain Controllers Explorer Summary (All DCs) view

The Domain Controllers Explorer Summary (All DCs) view displays more detailed resource metrics and information about all of the monitored DCs in your Active Directory® environment.

Figure 33. Domain Controllers Explorer Summary (All DCs) view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 From the Active Directory Enterprise view (under Dashboards in the navigation panel), select the **Domain Controllers object container**.

The Domain Controllers Explorer Summary (All DCs) view appears in the Primary view on the Active Directory Explorer dashboard.

NOTE: You can also click the view in Explorer link on the Domain Controllers Environment Summary (All DCs) view.

Embedded views

In addition to the current domain controller alarms, this view is made up of the following embedded views:

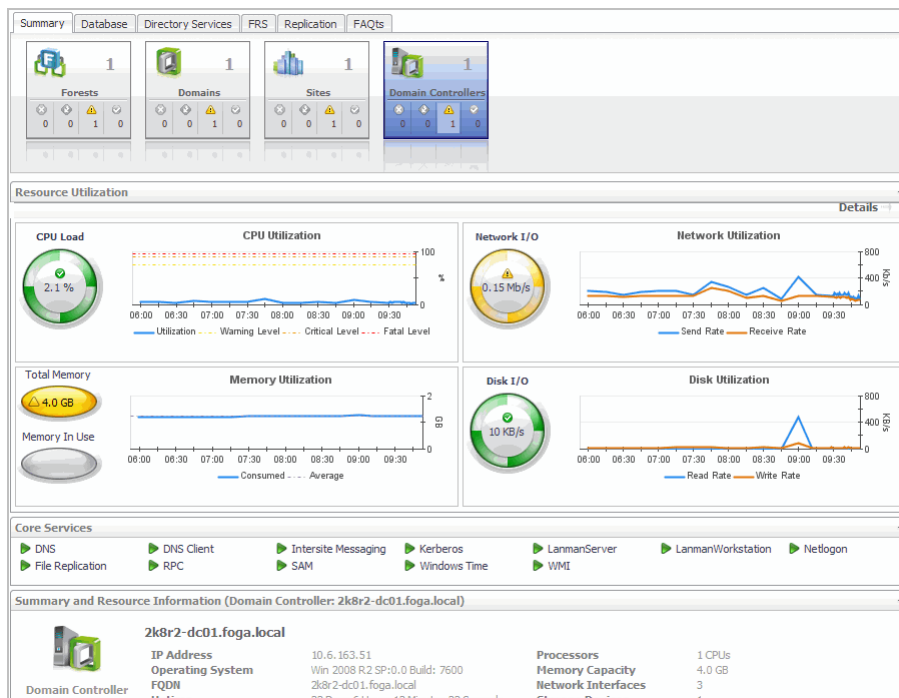
- [Top 3 CPU Consumers view](#)
- [Top 3 Memory Consumers view](#)
- [Top 3 Network Consumers view](#)
- [Top 3 Storage Consumers view](#)
- [Domain Controllers view](#)

Domain Controller Explorer Summary view

The Domain Controller Explorer Summary view displays more detailed resource metrics and information about the selected DC.

NOTE: If the resource utilization metrics and data are not appearing on this view, check the Host Collector setting on the agent's properties page. The VMWare option is selected by default. If Foglight for Active Directory, Foglight for Hyper-V, or Foglight for Infrastructure is being used to collect the host metrics, this setting must be set to the appropriate option.

Figure 34. Domain Controller Explorer Summary view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 Use one of the following methods to display this view:
 - From the Active Directory Enterprise view (under Dashboards in the navigation panel), select an individual **DC object**.
 - From the Domain Controllers tile (at the top of the Summary view), select the **Domain Controllers** icon, title or count. On the Domain Controllers Inventory dialog, select an individual **DC**.
- 3 Select the **Summary** navigation tab.

The Domain Controller Explorer Summary view appears in the Primary view on the Active Directory Explorer dashboard.

NOTE: You can also click the view in Explorer link on the Domain Controller Environment Summary view for the selected DC.

Embedded views

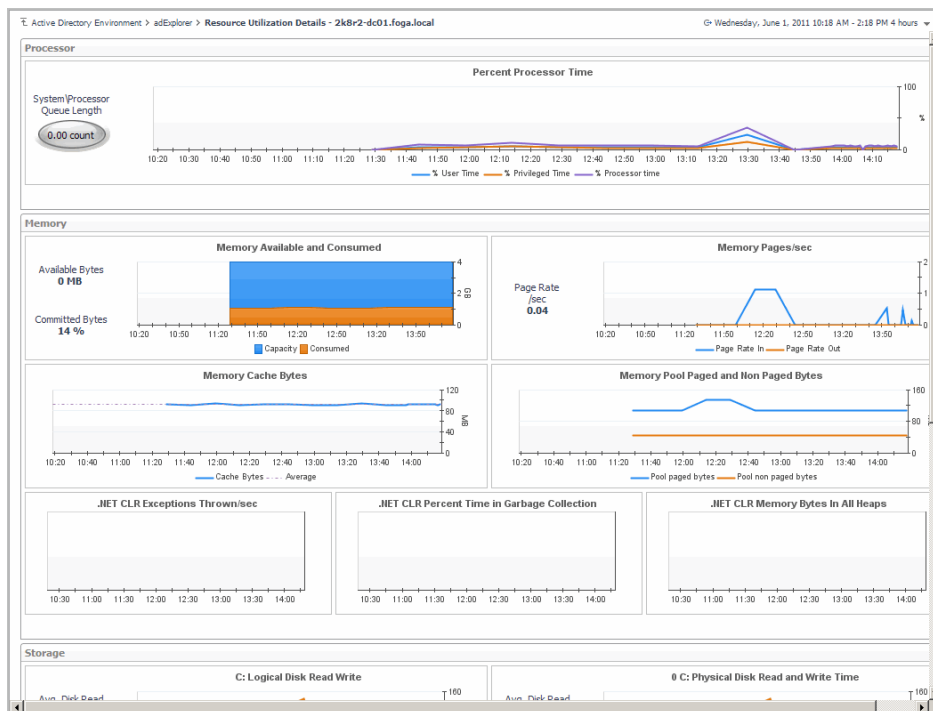
In addition to the current domain controller alarms, this view is made up of the following embedded views:

- [Resource Utilization view](#)
- [Asynchronous Thread Queue view](#)
- [Summary and Resource Information view](#)

Resource Utilization Details view

The Resource Utilization Details view displays more detailed information about the selected DC's resources.

Figure 35. Resource Utilization Details view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 Use one of the following methods to display this view:
 - From the Active Directory Enterprise view (under Dashboards in the navigation panel), select an individual **DC object**.
 - From the Domain Controllers tile (at the top of the Summary view), select the **Domain Controllers** icon, title or count. On the Domain Controllers Inventory dialog, select an individual **DC**.
- 3 Select the **Summary** navigation tab.
- 4 Click the **Resource Utilization** title or the **Details** link in the upper right-hand corner of the Resource Utilization view.

The Resource Utilization Details view appears in the Primary view on the Active Directory Explorer dashboard.

Embedded views

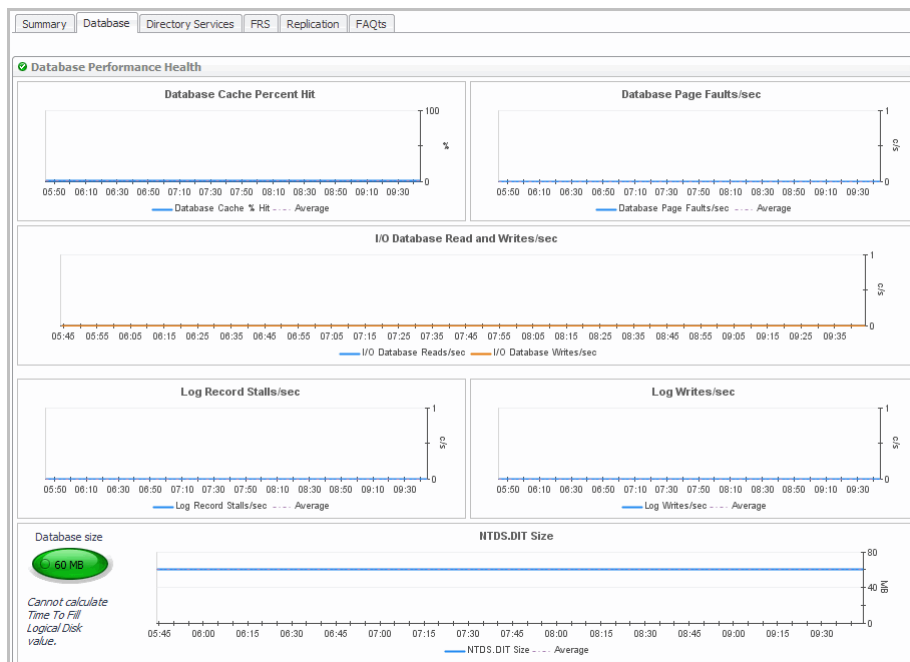
This view is made up of the following embedded views:

- [Processor view](#)
- [Memory view](#)
- [Storage view](#)
- [Network view](#)

Domain Controller Database view

The Domain Controller Database view displays performance health information about the selected DC's database.

Figure 36. Domain Controller Database view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 Use one of the following methods to display this view:
 - From the Active Directory Enterprise view (under Dashboards in the navigation panel), select an individual **DC object**.
 - From the Domain Controllers tile (at the top of the Summary view), select the **Domain Controllers** icon, title or count. On the Domain Controllers Inventory dialog, select an individual **DC**.
- 3 Select the **Database** navigation tab.

The Domain Controller Database view appears in the Primary view on the Active Directory Explorer dashboard.

Embedded views

This view is made up of the following embedded views:

- [Database Performance Health view](#)
- [Database Access view*](#)
- [Database Cache view*](#)
- [Database Log Access view*](#)
- [Defragmentation Tasks view*](#)

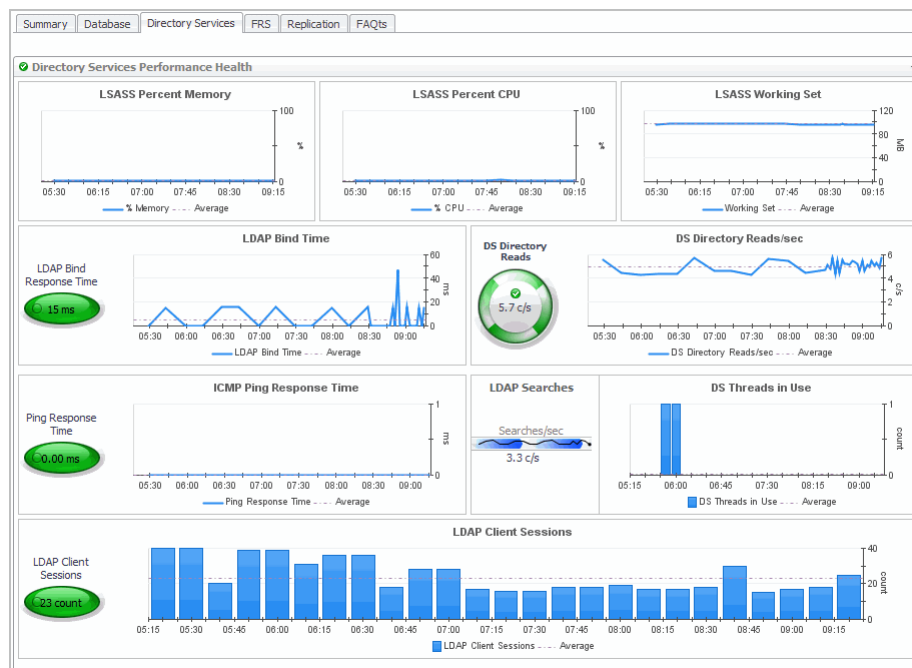
NOTE:

- i** **NOTE:** The views marked with an asterisk (*) are not displayed by default. In order to display these views, you must enable the corresponding collection group in the Database section of the Metrics Management dashboard.

Domain Controller Directory Services view

The Domain Controller Directory Services view displays performance health information about the selected DC's directory service processes.

Figure 37. Domain Controller Directory Services view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 Use one of the following methods to display this view:
 - From the Active Directory Enterprise view (under Dashboards in the navigation panel), select an individual **DC object**.
 - From the Domain Controllers tile (at the top of the Summary view), select the **Domain Controllers** icon, title or count. On the Domain Controllers Inventory dialog, select an individual **DC**.
- 3 Select the **Directory Services** navigation tab.

The Domain Controller Directory Services view appears in the Primary view on the Active Directory Explorer dashboard.

Embedded views

This view is made up of the following embedded views:

- [Directory Services General view](#)
- [Address Book view*](#)
- [Asynchronous Thread Queue view*](#)
- [Directory Services General view*](#)
- [Directory Services Reads view*](#)
- [Directory Services Searches view*](#)
- [Directory Services Writes view*](#)

- [Key Distribution Center view*](#)
- [LDAP view*](#)
- [Security Accounts Manager view*](#)

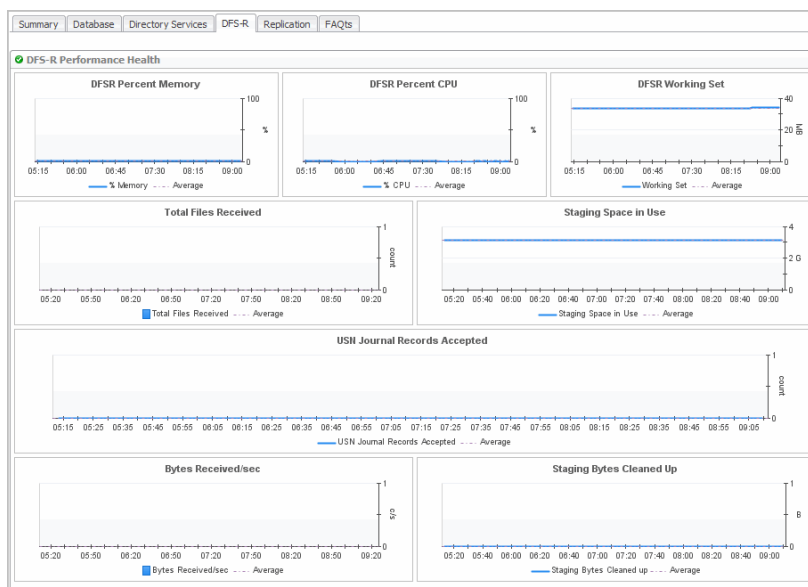
NOTE: The views marked with an asterisk (*) are not displayed by default. In order to display these views, you must enable the corresponding collection group in the Directory Services section of the Metrics Management dashboard.

Domain Controller DFS-R view

The Domain Controller DFS-R view displays performance health information about the selected DC's Distributed File System Replication (DFSR) service.

NOTE: Either the Domain Controller DFS-R view or the Domain Controller FRS view is displayed depending on the file replication service set up for the SYSVOL on the selected DC.

Figure 38. Domain Controller DFS-R view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 Use one of the following methods to display the Domain Controller Summary view:
 - From the Active Directory Enterprise view (under Dashboards in the navigation panel), select an individual **DC object**.
 - From the Domain Controllers tile (at the top of the Summary view), select the **Domain Controllers** icon, title or count. On the Domain Controllers Inventory dialog, select an individual **DC**.
- 3 Select the **DFS-R** navigation tab.

The Domain Controller DFS-R view appears in the Primary view on the Active Directory Explorer dashboard.

Embedded views

This view is made up of the following embedded views:

- [DFS Namespace Service API Queue view](#)

- DFS Namespace Service API Queue view*
- DFS Namespace Service API Requests view*
- DFS Namespace Service Referrals view*
- DFS Replicated Folders view*
- DFS Replication Connections view*
- DFS Replication Service Volumes view*

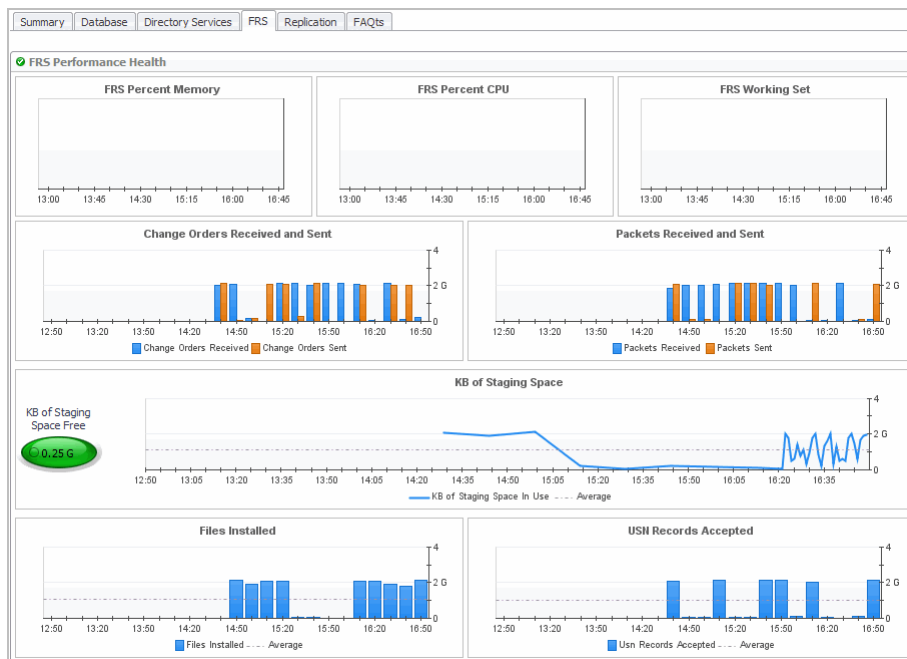
NOTE: The views marked with an asterisk (*) are not displayed by default. In order to display these views, you must enable the corresponding collection group in the DFS-R section of the Metrics Management dashboard.

Domain Controller FRS view

The Domain Controller FRS view displays performance health information about the selected DC's file replication service.

NOTE: Either the Domain Controller DFS-R view or the Domain Controller FRS view is displayed depending on the file replication service set up for the SYSVOL on the selected DC.

Figure 39. Domain Controller FRS view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 Use one of the following methods to display the Domain Controller Summary view:
 - From the Active Directory Enterprise view (under Dashboards in the navigation panel), select an individual **DC object**.
 - From the Domain Controllers tile (at the top of the Summary view), select the **Domain Controllers** icon, title or count. On the Domain Controllers Inventory dialog, select an individual **DC**.
- 3 Select the **FRS** navigation tab.

The Domain Controller FRS view appears in the Primary view on the Active Directory Explorer dashboard.

Embedded views

This view is made up of the following embedded view:

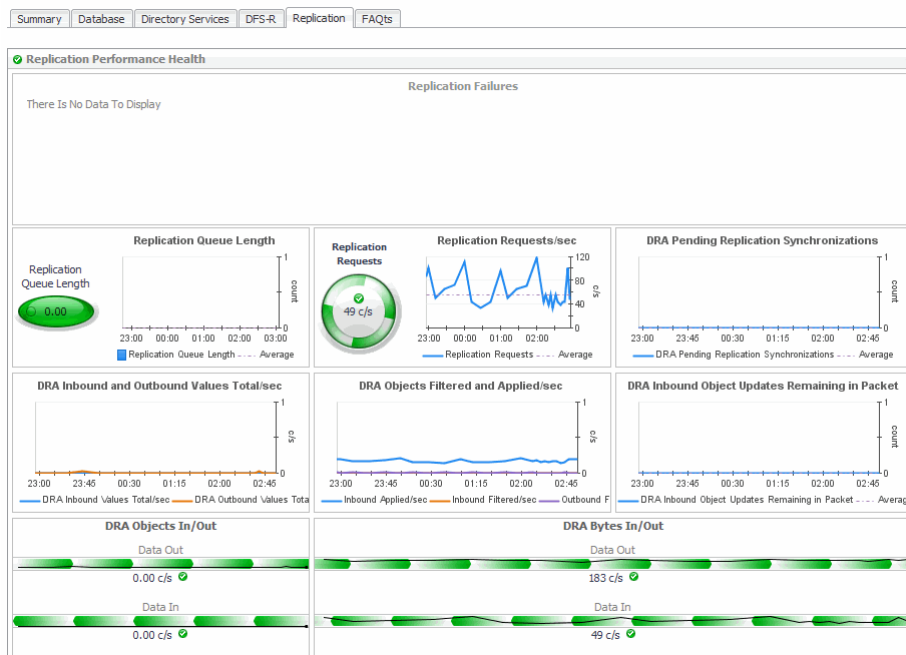
- [FRS Performance Health view](#)
- [FileReplicaConn Authentications/Bindings view*](#)
- [FileReplicaConn Change Orders view*](#)
- [FileReplicaConn Fetch view*](#)
- [FileReplicaSet Authentications/Bindings view*](#)
- [FileReplicaSet Change Orders view*](#)
- [FileReplicaSet DS Communications view*](#)
- [FileReplicaSet Files view*](#)
- [FileReplicaSet Local Change Orders view*](#)
- [FileReplicaSet Packets view*](#)
- [FileReplicaSet Remote Change Orders view*](#)
- [FRS Replica Sets view*](#)
- [FRS Staging Files view*](#)

NOTE: The views marked with an asterisk (*) are not displayed by default. In order to display these views, you must enable the corresponding collection group in the FRS section of the Metrics Management dashboard.

Domain Controller Replication view

The Domain Controller Replication view displays performance health information about the selected DC's replication activity.

Figure 40. Domain Controller Replication view



How to get here

- 1 From the Foglight navigation panel, select **Dashboards > Active Directory > Active Directory Explorer**.
- 2 Use one of the following methods to display the Domain Controller Summary view:
 - From the Active Directory Enterprise view (under Dashboards in the navigation panel), select an individual **DC object**.
 - From the Domain Controllers tile (at the top of the Summary view), select the **Domain Controllers** icon, title or count. On the Domain Controllers Inventory dialog, select an individual **DC**.
- 3 Select the **Replication** navigation tab.

The Domain Controller Replication view appears in the Primary view on the Active Directory Explorer dashboard.

Embedded views

This view is made up of the following embedded views:

- [Replication Performance Health view](#)
- [DFS Namespace Service API Queue view*](#)
- [Directory Replication Outbound view*](#)
- [Directory Replication Sync view*](#)
- [Directory Replication USN view*](#)

i **NOTE:** The views marked with an asterisk (*) are not displayed by default. In order to display these views, you must enable the corresponding collection group in the Replication section of the Metrics Management dashboard.

Description of embedded views

The remainder of this section provides a detailed description of the information and metrics presented in the embedded views introduced earlier in this section.

- [Address Book view](#)
- [Agent State view](#)
- [Asynchronous Thread Queue view](#)
- [Core Services view](#)
- [Database Access view](#)
- [Database Cache view](#)
- [Database Log Access view](#)
- [Database Performance Health view](#)
- [Defragmentation Tasks view](#)
- [DFS Namespace Service API Queue view](#)
- [DFS Namespace Service API Requests view](#)
- [DFS Namespace Service Referrals view](#)
- [DFS Replicated Folders view](#)
- [DFS Replication Connections view](#)
- [DFS Replication Service Volumes view](#)

- [DFS-R Performance Health view](#)
- [Directory Replication Inbound view](#)
- [Directory Replication Outbound view](#)
- [Directory Replication Sync view](#)
- [Directory Replication USN view](#)
- [Directory Services General view](#)
- [Directory Services Performance Health view](#)
- [Directory Services Reads view](#)
- [Directory Services Searches view](#)
- [Directory Services Writes view](#)
- [Domain Controller Details view](#)
- [Domain Controllers view](#)
- [FileReplicaConn Authentications/Bindings view](#)
- [FileReplicaConn Change Orders view](#)
- [FileReplicaConn Fetch view](#)
- [FileReplicaSet Authentications/Bindings view](#)
- [FileReplicaSet Change Orders view](#)
- [FileReplicaSet DS Communications view](#)
- [FileReplicaSet Files view](#)
- [FileReplicaSet Local Change Orders view](#)
- [FileReplicaSet Packets view](#)
- [FileReplicaSet Remote Change Orders view](#)
- [FRS Performance Health view](#)
- [FRS Replica Sets view](#)
- [FRS Staging Files view](#)
- [FSMO Roles view \(Domain\)](#)
- [FSMO Roles view \(Forest\)](#)
- [Host Monitor view](#)
- [Inter-Site Transports view](#)
- [Inventory By Category view](#)
- [IP Subnets view](#)
- [Key Distribution Center view](#)
- [LDAP view](#)
- [Memory view](#)
- [Network view](#)
- [Processor view](#)
- [Replication Performance Health view](#)
- [Resource Utilization view](#)
- [Security Accounts Manager view](#)
- [Server Health view](#)

- [Statistics view](#)
- [Storage view](#)
- [Summary and Resource Information view](#)
- [Top AD Metrics view](#)
- [Top 3 Consumers view](#)
- [Top 3 CPU Consumers view](#)
- [Top 3 DS Directory Reads/sec view](#)
- [Top 3 LDAP Bind Times view](#)
- [Top 3 Memory Consumers view](#)
- [Top 3 Network Consumers view](#)
- [Top 3 Replication Queue Length view](#)
- [Top 3 Storage Consumers view](#)
- [Trusts view](#)
- [USN Records view](#)

Address Book view

To display this view, enable the **Address Book Group** in the Directory Services section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Directory Services navigation tab for the selected domain controller in the Active Directory Explorer dashboard.

Table 13. Address Book view

Description	This view displays Address Book (AB) metrics for the selected server which are gathered when the Address Book collection group is enabled.
Data displayed	<p>AB ANR/sec. This counter shows the rate at which Address Book clients perform Ambiguous Name Resolution (ANR) operations per second.</p> <p>AB Client Sessions. This counter shows the number of connected Address Book client sessions.</p> <p>AB Browsers/sec. This counter shows the rate at which Address Book clients perform browse operations per second.</p> <p>AB Matches/sec. This graph charts the rate at which Address Book clients perform find operations per second. It provides a comparison against the computed average for the specified time interval.</p> <p>AB Property Reads, Proxy Lookups and Searches/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • AB Property Reads/sec. Shows the rate at which Address Book clients perform read operations per second. • AB Proxy Lookups/sec. Shows the rate at which proxy clients perform search operations per second. • AB Searches/sec. Shows the rate at which Address Book clients perform key search operations per second.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Agent State view

This embedded view is part of the Domain Controller Environment Summary for an individual DC in the Active Directory Environment dashboard.

Table 14. Agent State view

Description	This view displays the current status of the agent hosting the selected DC.
Where to go next	Drill down on: <ul style="list-style-type: none">• State Icon. Displays a popup listing the current alarms.• Agent Link (arrow). Displays the Agents on All Hosts dashboard which lists the agents that are available for each host. This dashboard also displays health history and the outstanding alarms for all monitored hosts and agents. For more information about this dashboard, see <i>Investigating Problems with Agents</i> in the <i>Foglight User Help</i>.

Asynchronous Thread Queue view

To display this view, enable the **Asynchronous Thread Queue Group** in the Directory Services section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Directory Services navigation tab for the selected domain controller in the Active Directory Explorer dashboard.

Table 15. Asynchronous Thread Queue view

Description	This view displays Asynchronous Thread Queue (ATQ) metrics for the selected DC which are gathered when the Asynchronous Thread Queue collection group is enabled.
Data displayed	Asynchronous Threads. This graph charts the following metrics: <ul style="list-style-type: none">• ATQ Threads LDAP. Shows the number of threads that ATQ has currently allocated to servicing LDAP requests.• ATQ Threads Other. Shows the number of threads that ATQ has currently allocated to DS services other than LDAP.• ATQ Threads Total. Shows the total number ATQ threads that are either waiting to service an incoming request or are already servicing a request.
Where to go next	Drill down on: <ul style="list-style-type: none">• Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Core Services view

To display this view, select the **Summary** navigation tab for an individual DC in the Active Directory Explorer dashboard. This embedded view is located below the Resource Utilization view in the Primary view.

Table 16. Core Services view

Description	<p>This view displays a list of the core services that are being monitored and their present state. The following symbols are used to illustrate the current state of a service:</p> <ul style="list-style-type: none"> • green arrow - service is running on the server • red square - service is not running on the server • gray circle with ? - status of the service is unknown; has a status other than running or not running; could possible mean the service is not found on the server <p>NOTE: This list corresponds to the Monitored Services list assigned to the selected DC (Agent Properties).</p>
Where to go next	N/A

Database Access view

To display this view, enable the **Database Access Group** in the Database section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Database navigation tab for the selected domain controller in the Active Directory Explorer dashboard.

Table 17. Database Access view

Description	<p>This view displays additional database access metrics for the selected DC which are gathered when the Database Access collection group is enabled.</p>
Data displayed	<p>I/O Database Average Latency. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • I/O Database Reads Average Latency. Shows the average length of time it takes to perform a database read operation. • I/O Database Writes Average Latency. Shows the average length of time it takes to perform a write operation. <p>Database Page Evictions and Fault Stalls/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Database Page Evictions/sec. Shows the rate at which database file page requests require the database cache manager to allocate a new page from the database cache forcing another database page out of the cache. • Database Page Stalls/sec. Shows the rate at which page faults cannot be serviced because there are no pages available for allocation from the database cache. <p>Pages and Records Converted. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Pages Converted. Shows the number of database pages that have been converted from an older format. • Records Converted. Shows the number of database records that have been converted from an older format. <p>Pages and Records Converted/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Pages Converted/sec. Shows the number of times per second that a database page is converted from an older database format. • Records Converted/sec. Shows the number of times per second that a database record is converted from an older database format. <p>Sessions in Use. This counter shows the number of database sessions currently open for use by client threads.</p> <p>Sessions % Used. This counter shows the percentage of database sessions currently open for use by client threads.</p> <p>Version Buckets Allocated. This counter shows the total number of version buckets allocated.</p>

Table 17. Database Access view

	Table Opens/sec. This counter shows the number of database tables opened per second.
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Database Cache view

To display this view, enable the **Database Cache Group** in the Database section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Database navigation tab for the selected domain controller in the Active Directory Explorer dashboard.

Table 18. Database Cache view

Description	This view displays additional database cache metrics for the selected DC which are gathered when the Database Cache collection group is enabled.
Data displayed	<p>Database Cache/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none"> Database Cache Misses/sec. Shows the rate at which database file page requests are fulfilled by the database cache by causing a file operation. Database Cache Requests/sec. Shows the rate at which pages are requested from the database cache. <p>Database Cache Size (MB). This graph charts the following metrics:</p> <ul style="list-style-type: none"> Database Cache Size (MB). Shows the amount of system memory (in MB) used by the database cache manager to hold commonly used information from the database file(s) to prevent file operations. Database Cache Size Resident (MB). Shows the amount of system memory (in MB) used by the database cache manager that is currently part of the working set of the process. <p>Database Cache Size. This counter displays the amount of system memory used by the database cache manager to hold commonly used information from the database file(s) to prevent file operations.</p> <p>Database Cache Size Resident. This counter displays the amount of system memory used by the database cache manager that is currently part of the working set of the process.</p> <p>Table Open Cache Hits/sec. This counter shows the number of database tables opened per second by using cached schema information.</p> <p>Table Open Cache Misses/sec. This counter shows the number of database tables opened per second without using cached schema information.</p> <p>Table Open Cache % Hit. This counter shows the percentage of database tables opened using cached schema information.</p>
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Database Log Access view

To display this view, enable the **Database Log Access Group** in the Database section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Database navigation tab for the selected domain controller in the Active Directory Explorer dashboard.

Table 19. Database Log Access view

Description	This view displays additional database log access metrics for the selected DC which are gathered when the Database Log Access collection group is enabled.
Data displayed	<p>I/O Log Reads and Writes/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • I/O Log Reads/sec. Shows the rate at which log file read operations are completed. • I/O Log Writes/sec. Shows the rate at which log file write operations are completed. <p>I/O Log Writes Average Latency. This graph charts the average length of time it takes to perform a log file write operation. It provides a comparison against the computed average for the specified time interval.</p> <p>Log Bytes Generated and Writes/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Log Bytes Generated/sec. Shows the rate at which data is added to the log. • Log Bytes Write/sec. Shows the rate at which bytes are written to the log. <p>Log Threads Waiting. This graph charts the number of threads waiting on pending log writes. It provides a comparison against the computer average for the specified time interval.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Database Performance Health view

To display this embedded view, select the **Database** navigation tab for an individual DC in the Active Directory Explorer dashboard.

Table 20. Database Performance Health view

Description	This view displays the database performance metrics for the selected DC. These counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	<p>Database Cache Percent Hit. This graph charts the percent of database page requests handled by the cache for the selected DC. It provides a comparison against the computed average for the specified time interval.</p> <p>Database Page Faults/sec. This graph charts the rate at which the database file page requests require the database cache manager to allocate a new page from the database cache. It provides a comparison against the computed average for the specified time interval.</p> <p>I/O Database Reads and Writes/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • I/O Database Reads/sec. Shows the rate at which database read operations completed. • I/O Database Writes/sec. Shows the rate at which database write operations completed. <p>Log Record Stalls/sec. This graph charts the number of log records (per second) that could not be added to the log buffers because the buffers were full. It provides a comparison against the computed average for the specified time interval.</p> <p>Log Writes/sec. This graph charts the number of times the log buffers are written to the log file per second. It provides a comparison against the computed average for the specified time interval.</p> <p>Database Size. This button displays the current size of the Active Directory® database.</p>

Table 20. Database Performance Health view

	NTDS.DIT Size. This graph charts the size (in MB) of the database on the selected DC. It provides a comparison against the computed average for the specified time interval.
Where to go next	Drill down on: <ul style="list-style-type: none"> • Database Performance title - displays an Alarms popup listing the current Database alarms that are outstanding for the selected DC. • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Defragmentation Tasks view

To display this view, enable the **Defragmentation Tasks Group** in the Database section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Database navigation tab for the selected domain controller in the Active Directory Explorer dashboard.

Table 21. Defragmentation Tasks view

Description	This view displays database defragmentation task metrics for the selected DC which are gathered when the Defragmentation Tasks collection group is enabled.
Data displayed	Defragmentation Tasks. This graph charts the following metrics: <ul style="list-style-type: none"> • Defragmentation Tasks. Shows the number of background database defragmentation tasks that are currently executing. • Defragmentation Tasks Pending. Shows the number of background database defragmentation tasks that are currently pending.
Where to go next	Drill down on: <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

DFS Namespace Service API Queue view

To display this view, enable the **DFS Namespace Service API Queue Group** in the DFS-R section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the DFS-R navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 22. DFS Namespace Service API Queue view

Description	This view displays metrics related to the DFS Namespace Service API queues for the selected DC which are gathered when the DFS Namespace Service API Queue collection group is enabled.
Data displayed	NetDfs API Queue Length. This graph charts the number of API call requests waiting to be processed by the service. It provides a comparison against the computed average for the specified time interval.
Where to go next	Drill down on: <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

DFS Namespace Service API Requests view

To display this view, enable the **DFS Namespace Service API Requests Group** in the DFS-R section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the DFS-R navigation tab in the Active Directory Explorer dashboard.

NOTE: Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 23. DFS Namespace Service API Requests view

Description	This view displays metrics related to the DFS Namespace Service API requests for the selected DC which are gathered when the DFS Namespace Service API Requests collection group is enabled.
Data displayed	<p>Average Response Time. This graph charts the average response time it takes for a request to one API to be processed by the DFS Namespace service. It provides a comparison against the computed average for the specified time interval.</p> <p>Requests Processed/sec. This graph charts the number of API requests that are being processed per second by the DFS Namespace service. It provides a comparison against the computed average for the specified time interval.</p> <p>Requests Processed and Failed. This graph charts the following metrics:</p> <ul style="list-style-type: none">• Requests Failed. Shows the number of requests to one API that failed when being processed by the DFS Namespace service.• Requests Processed. Shows the number of requests on one API that were successfully processed by the DFS Namespace service.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

DFS Namespace Service Referrals view

To display this view, enable the **DFS Namespace Service Referrals Group** in the DFS-R section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the DFS-R navigation tab in the Active Directory Explorer dashboard.

NOTE: Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 24. DFS Namespace Service Referrals view

Description	This view displays metrics related to the DFS Namespace Service referrals for the selected DC which are gathered when the DFS Namespace Service Referrals collection group is enabled.
Data displayed	<p>Average Response Time. This graph charts the average response time it takes for a referral request to be processed by the DFS Namespace service. It provides a comparison against the computed average for the specified time interval.</p> <p>Requests Processed/sec. This graph charts the number of referral requests that are being processed per second by the DFS Namespace service. It provides a comparison against the computed average for the specified time interval.</p>

Table 24. DFS Namespace Service Referrals view

<p>Requests Processed and Failed. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Requests Failed. Shows the number of referral requests that failed when being processed by the DFS Namespace service. • Requests Processed. Shows the number of referral requests that were successfully processed by the DFS Namespace service. 	
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

DFS Replicated Folders view

To display this view, enable the **DFS Replicated Folders Group** in the DFS-R section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the DFS-R navigation tab in the Active Directory Explorer dashboard.

NOTE: Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 25. DFS Replicated Folders view

Description	This view displays replicated folder metrics associated with the DFS Replication service on the selected DC which are gathered when the DFS Replicated Folders collection group is enabled.
Data displayed	<p>Bandwidth Savings Using DFS Replication. This counter shows the percentage of bandwidth that was saved by the DFS Replication service for the selected replicated folder.</p> <p>Compressed Size of Files Received. This counter shows the compressed size (in bytes) of files received for the selected replicated folder.</p> <p>Size of Files Received. This counter shows the uncompressed size (in bytes) of the files received for the selected replicated folder.</p> <p>Space in Use. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> • Conflict Space in Use. Shows the amount of space (in bytes) being used by conflict loser files and folders currently in the Conflict and Deleted folder. • Deleted Space in Use. Shows the amount of space (in bytes) being used by deleted files and folders currently in the Conflict and Deleted folder. <p>Deleted Files. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> • Deleted Files Cleaned Up. Shows the number of replicated deleted files and folders that were cleaned up from the Conflict and Deleted folder. • Deleted Files Generated. Shows the number of replicated deleted files and folders that were moved to the Conflict and Deleted folder. <p>Deleted Bytes. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> • Deleted Bytes Cleaned Up. Shows the total amount of space (in bytes) from replicating deleted files and folders that were cleaned up from the Conflict and Deleted folder. • Deleted Bytes Generated. Shows the total amount of space (in bytes) from replicated deleted files and folders that were moved to the Conflict and Deleted folder. <p>Updates Dropped. This graph charts the number of redundant file replication update records that were ignored. It provides a comparison against the computed average for the specified time interval.</p>

Table 25. DFS Replicated Folders view

	<p>Files Installed. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> • File Installs Succeeded. Shows the number of files successfully received from sending members and installed locally on the selected server. • File Installs Retried. Shows the number of files that are being retried due to sharing violations or other errors encountered when installing the files.
	<p>RDC Bytes Received. This graph charts the number of bytes that were received in replicating files using remote differential compression (RDC) for the selected replicated folder. It provides a comparison against the computed average for the specified time interval.</p>
	<p>RDC Size of Files. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> • RDC Compressed Size of Files Received. Shows the number of bytes that would have been received had RDC not been used. • RDC Size of Files Received. Shows the number of bytes that would have been received had neither compression or RDC been used.
	<p>RDC Number of Files Received. This graph charts the number of files that were received for the selected replicated folder. It provides a comparison against the computed average for the specified time interval.</p>
	<p>Conflict Bytes Cleaned Up. This counter shows the total size (in bytes) of conflict loser files and folders that were deleted from the Conflict and Deleted folder.</p>
	<p>Conflict Bytes Generated. This counter shows the total size (in bytes) of files and folders in the selected replicated folder that were moved to the Conflict and Deleted folder.</p>
	<p>Conflict Files Cleaned Up. This counter shows the number of conflict loser files and folders that were deleted from the Conflict and Deleted folder.</p>
	<p>Conflict Files Generated. This counter shows the number of files and folders in the selected replicated folder that were moved to the Conflict and Deleted folder.</p>
	<p>Conflict Folder Cleanups Completed. This counter shows the number of times conflict loser files and folders were deleted from the Conflict and Deleted folder.</p>
	<p>Staging Bytes Generated. This counter shows the total size (in bytes) of replicated files and folders in the Staging folder.</p>
	<p>Staging Files Cleaned Up. This counter shows the number of files and folders that were cleaned up from the Staging folder.</p>
	<p>Staging Files Generated. This counter shows the number of times replicated files and folders were staged.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

DFS Replication Connections view

To display this view, enable the **DFS Replication Connections Group** in the DFS-R section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the DFS-R navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 26. DFS Replication Connections view

Description	This view displays connection metrics associated with the DFS Replication service for the selected DC which are gathered when the DFS Replication Connections collection group is enabled.
Data displayed	<p>Compressed Size of Files Received. This counter shows the compressed size (in bytes) of the files received on the connection.</p> <p>Size of Files Received. This counter shows the uncompressed size (in bytes) of the files received on the connection.</p> <p>Total Files Received. This counter shows the total number of files received on the connection.</p> <p>Total Bytes Received. This counter shows the total number of bytes received on the connection.</p> <p>Bandwidth Savings Using DFS Replication. This graph charts the percentage of bandwidth that was saved by the DFS Replication service.</p> <p>RDC Number of Files Received. This graph charts the number of files that were received on the connection while replicating files using Remote Differential Compression (RDC).</p> <p>RDC Bytes Received. This graph charts the number of bytes that were received on the connection while replicating files using RDC.</p> <p>RDC Size of Files. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> RDC Size of Files Received. Shows the uncompressed size (in bytes) of files received with RDC for the connection. RDC Compressed Size of Files Received. Shows the compressed size (in bytes) of files received with RDC for the connection.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

DFS Replication Service Volumes view

To display this view, enable the **DFS Replication Service Volumes Group** in the DFS-R section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the DFS-R navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 27. DFS REplication Service Volumes view

Description	This view displays volume metrics associated with the DFS Replication service for the selected DC which are gathered when the DFS Replication Service Volumes collection group is enabled.
Data displayed	<p>Database Commits. This graph charts the number of database commit operations performed by the DFS Replication service. It provides a comparison against the computed average for the specified time interval.</p> <p>Database Lookups. This graph charts the number of database search operations performed by the DFS Replication service. It provides a comparison against the computed average for the specified time interval.</p>

Table 27. DFS REplication Service Volumes view

	USN Journal Records Read. This graph charts the number of USN journal records that were read by the DFS Replication service. It provides a comparison against the computed average for the specified time interval.
	USN Journal Unread Percentage. This graph charts the percentage of the USN journal that has not yet been read and processing by the DFS Replication service.
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

DFS-R Performance Health view

To display this embedded view, select the **DFS-R** navigation tab for an individual DC in the Active Directory Explorer dashboard.

NOTE: Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 28. DFS-R Performance Health view

Description	This view displays the Distributed File System Replication (DFSR) service performance metrics for the selected DC. These counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	<p>DFSR Percent Memory. This graph charts the percent of memory being consumed by the DFSRS process on the selected DC over the specified time interval.</p> <p>DFSR Percent CPU. This graph charts the percent of CPU being consumed by the DFSRS process on the selected DC.</p> <p>DFSR Working Set. This graph charts the number of memory pages recently used by the threads in the DFSRS process on the selected DC.</p> <p>Bytes Received/sec. This graph charts the estimated average number of bytes that were received by this replicated folder each second over the past 30 seconds. It provides a comparison against the computer average for the specified time interval.</p> <p>Staging Space in Use. This graph charts the amount of space (in bytes) being used for files and folders currently in the staging folder. It provides a comparison against the computed average for the specified time interval.</p> <p>USN Journal Records Accepted. This graph charts the number of Update Sequence Number (USN) records that were processed by the DRS replication service. It provides a comparison against the computed average for the specified time interval.</p> <p>File Installs Retrieved. This graph charts the number of bytes that were received in replicating files using remote differential compression (RDC) for the selected replicated folder. It provides a comparison against the computed average for the specified time interval.</p> <p>Staging Bytes Cleaned Up. This graph charts the amount of space (in bytes) being used for files and folders that were cleaned up from the staging folder. It provides a comparison against the computed average for the specified time interval.</p>
Where to go next	Drill down on: <ul style="list-style-type: none"> DFS-R Performance Health title - displays an Alarms popup listing the current DFS-R alarms that are outstanding for the selected DC. Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Directory Replication Inbound view

To display this view, enable the **Directory Replication Inbound Group** in the Replication section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Replication navigation tab in the Active Directory Explorer dashboard.

Table 29. Directory Replication Inbound view

Description	This view displays additional inbound replication metrics for the selected DC which are gathered when the Directory Replication Inbound collection group is enabled.
Data displayed	<p>DRA Inbound Bytes Compressed. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DRA Inbound Bytes Compressed (Between Sites, After Compression). Shows the compressed size (in bytes) of inbound compressed replication data (size after compression from DSAs in other sites).• DRA Inbound Bytes Compressed (Between Sites, Before Compression). Shows the original size (in bytes) of inbound compressed replication data. <p>DRA Inbound Bytes Compressed/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DRA Inbound Bytes Compressed (Between Sites, After Compression)/sec. Shows the compressed size (in bytes) of inbound compressed replication data per second.• DRA Inbound Bytes Compressed (Between Sites, Before Compression)/sec. Shows the original size (in bytes) of inbound compressed replication data per second. <p>DRA Inbound Bytes Not Compressed (Within Site)/sec. This graph charts the number of bytes replicated in that were not compressed at the source (from DSAs in the same site) per second. It provides a comparison against the computed average for the specified time interval.</p> <p>DRA Inbound Bytes Not Compressed (Within Site). This graph charts the number of bytes replicated in that were not compressed at the source (from DSAs in the same site). It provides a comparison against the computed average for the specified time interval.</p> <p>DRA Inbound Full Sync Objects Remaining. This graph charts the number of objects remaining until the full sync completes. It provides a comparison against the computed average for the specified time interval.</p> <p>DRA Inbound Link Value Updates Remaining in Packet. This graph charts the number of link value updates received in the current directory replication update packet that have not yet been applied to the local server. It provides a comparison against the computed average for the specified time interval.</p> <p>DRA Inbound Properties Applied/sec. This counter shows the number of properties that are updated due to the incoming property winning the reconciliation logic that determines the final value to be replicated.</p> <p>DRA Inbound Properties Filtered/sec. This counter shows the number of property changes that are received during the replication that have not yet been seen.</p> <p>DRA Inbound Properties Total/sec. This counter shows the total number of object properties received from inbound replication partners.</p> <p>DRA Inbound Values (DNs only)/sec. This counter shows the number of object property values received from inbound replication partners that are Distinguished Names (DNs) that reference other objects.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Directory Replication Outbound view

To display this view, enable the **Directory Replication Outbound Group** in the Replication section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Replication navigation tab in the Active Directory Explorer dashboard.

Table 30. Directory Replication Inbound view

Description	This view displays additional outbound replication metrics for the selected DC which are gathered when the Directory Replication Outbound collection group is enabled.
Data displayed	<p>DRA Outbound Bytes Compressed. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DRA Outbound Bytes Compressed (Between Sites, After Compression). Shows the compressed size (in bytes) of outbound compressed replication data (size after compression from DSAs in other sites).• DRA Outbound Bytes Compressed (Between Sites, Before Compression). Shows the original size (in bytes) of outbound compressed replication data (size before compression from DSAs in others sites). <p>DRA Outbound Bytes Compressed/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DRA Outbound Bytes Compressed (Between Sites, After Compression)/sec. Shows the compressed size (in bytes) of outbound compressed replication data per second.• DRA Outbound Bytes Compressed (Between Sites, Before Compression)/sec. Shows the original size (in bytes) of outbound compressed replication data per second. <p>DRA Outbound Bytes Not Compressed (Within Site)/sec. This graph charts the number of bytes replicated out that were not compressed (that is, from DSAs in the same site) per second. It provides a comparison against the computed average for the specified time interval.</p> <p>DRA Outbound Bytes Not Compressed (Within Site). This graph charts the number of bytes replicated out that were not compressed (that is, from DSAs in the same site). It provides a comparison against the computed average for the specified time interval.</p> <p>DRA Outbound Bytes Total Since Boot. This graph charts the total number of bytes replicated out. It includes the number of uncompressed bytes (never compressed) and compressed bytes (after compression). It provides a comparison against the computed average for the specified time interval.</p> <p>DRA Outbound Properties and Values. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DRA Outbound Properties/sec. Shows the number of properties replicated out per second.• DRA Outbound Values (DNs only)/sec. Shows the number of object property values containing Distinguished Names (DNs) sent to outbound replication partners per second.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Directory Replication Sync view

To display this view, enable the **Directory Replication Sync Group** in the Replication section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Replication navigation tab in the Active Directory Explorer dashboard.

Table 31. Directory Replication Sync view

Description	This view displays additional replication synchronization metrics for the selected DC which are gathered when the Directory Replication Sync collection group is enabled.
Data displayed	<p>DRA Pending Replication Operations. This counter shows the total number of replication operations on the directory that are queued for the selected server but not yet performed.</p> <p>DRA Sync Failures on Schema Mismatch. This counter shows the number of sync requests made to the neighbors that failed because their schema are out of sync.</p> <p>DRA Sync Requests Successful. This counter shows the number of sync requests made to the neighbors that successfully returned.</p> <p>DRA Threads Getting NC Changes. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • DRA Threads Getting NC Changes. Shows the number of threads on the selected server that are currently attempting to acquire changes from another server. • DRA Threads Getting NC Changes Holding Semaphore. Shows the number of threads on the selected server that are currently attempting to acquire changes from another server and hold a semaphore required to get these changes. <p>DRA Sync Requests Made. This graph charts the number of directory synchronization requests made to the neighbors. It provides a comparison against the computed average for the specified time interval.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Directory Replication USN view

To display this view, enable the **Directory Replication USN Group** in the Replication section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Replication navigation tab for the selected DC in the Active Directory Explorer dashboard.

Table 32. Directory Replication USN view

Description	This view displays additional metrics about the DRA highest USNs for the selected DC which are gathered when the Directory Replication USN collection group is enabled.
Data displayed	<p>DRA Highest USN Committed. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • DRA Highest USN Committed (High part). Shows the high-order 32 bits of the highest USN committed on the DSA. • DRA Highest USN Committed (Low part). Shows the low-order 32 bits of the highest USN committed on the DSA. <p>DRA Highest USN Issued. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • DRA Highest USN Issued (High part). Shows the high-order 32 bits of the highest USN issued on the DSA. <p>DRA Highest USN Issued (Low part). Shows the low-order 32 bits of the highest USN issued on the DSA.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Directory Services General view

To display this view, enable the **Directory Services General Group** in the Directory Services section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Directory Services navigation tab for the selected DC in the Active Directory Explorer dashboard.

Table 33. Directory Services General view

Description	This view displays additional directory service metrics for the selected DC which are gathered when the Directory Services General collection group is enabled.
Data displayed	<p>DS Client Bind and Name Translations/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DS Client Binds/sec. Shows the number of NTDSAPI.DLL binds serviced by the selected DC per second.• DS Client Name Translations/sec. Shows the number of NTDSAPI.DLL name translations serviced by the selected DC per second. <p>DS Directory Searches and Writes/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DS Directory Searches/sec. Shows the number of directory searches performed per second.• DS Directory Writes/sec. Shows the number of directory writes performed per second. <p>DS Monitor List. This graph charts the number of requests to be notified when objects are updated that are currently registered with the DSA. It provides a comparison against the computed average for the specified time interval.</p> <p>DS Name Cache Hit Rate. This graph charts the percentage of directory object name component look ups that are satisfied out of the DSA's name cache.</p> <p>DS Notify Queue Size. This graph charts the number of pending update notifications that have been queued, but not yet transmitted to clients. It provides a comparison against the computed average for the specified time interval.</p> <p>DS Security Descriptor Propagation. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DS Security Descriptor Propagation Events. Shows the number of Security Descriptor Propagation events that are queued but not yet processed.• DS Security Descriptor Propagator Average Exclusion. Shows the average length of time the Security Descriptor propagator spends waiting for exclusive access to database elements during a Security Descriptor Propagation sub-operation.• DS Security Descriptor Propagator Runtime Queue. Shows the number of objects remaining to be examined while processing the current DS Security Descriptor Propagator event.• DS Security Descriptor Sub-Operations/sec. Shows the number of Security Descriptor propagation sub-operations performed per second. <p>DS Search Sub-Operations/sec. This graph charts the number of search sub-operations performed per second.</p> <p>NOTE: One search operation may be made up of many sub-operations.</p> <p>DS Server Name Translations/sec. This button shows the number of DC-to-DC name translations serviced by the selected DC per second.</p> <p>DS Server Binds and Name Translations/sec. This graph charts the number of DC-to-DC binds serviced by the selected DC per second. It provides a comparison against the computed average for the specified time interval.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Directory Services Performance Health view

To display this embedded view, select the **Directory Services** navigation tab for an individual DC in the Active Directory Explorer dashboard.

Table 34. Directory Services Performance Health view

Description	This view displays directory services performance metrics for the selected DC. The counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	LSASS Percent Memory. This graph charts the percent of memory being consumed by the LSASS process on the selected DC.
	LSASS Percent CPU. This graph charts the percent of CPU being consumed by the LSASS process on the selected DC.
	LSASS Working Set. This graph charts the number of memory page sets recently used by the threads in the LSASS process.
	LDAP Bind Response Time. This button shows the amount of time it took (in milliseconds) to complete the last LDAP bind request.
	LDAP Bind Time. This graph charts the LDAP bind time, in milliseconds. It provides a comparison against the computed average for the specified time interval.
	DS Directory Reads. This counter displays the rate at which directory read operations are being performed per second.
	DS Directory Reads/sec. This graph charts the number of directory read operations performed per second. It provides a comparison against the computed average for the specified time interval.
	Kerberos Authentications. This counter displays the rate at which clients are using a Kerberos ticket to authenticate to the DC. NOTE: This metric applies to Windows 2003 only.
	Authentication Requests. This graph displays the number of times per second that clients use a Kerberos ticket to authenticate to the DC. NOTE: This metric applies to Windows 2003 only.
	Ping Response Time. This button shows the ping time, or average round trip time, it is taking for packets from the local host to reach the designated computer.
	ICMP Ping Response Time. This graph charts the round trip time it took for packets from the local host to reach designated computers. It provides a comparison against the computed average for the specified time interval.
	LDAP Searches. This pulse gauge displays the rate at which LDAP clients perform search operations per second.
Where to go next	DS Threads in Use. This graph charts the number of threads currently servicing client API calls. It provides a comparison against the computed average for the specified time interval.
	LDAP Client Sessions. The button shows the number of clients that currently have open LDAP sessions with the DC. The graph charts the number of clients that have open LDAP sessions with the selected DC. It provides a comparison against the computed average for the specified time interval.
	Drill down on: <ul style="list-style-type: none">• Directory Services Performance title - displays an Alarms popup listing the current Directory Services alarms that are outstanding for the selected DC.• Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Directory Services Reads view

To display this view, enable the **Directory Services Reads Group** in the Directory Services section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Directory Services navigation tab for the selected DC in the Active Directory Explorer dashboard.

Table 35. Directory Services Reads view

Description	This view displays additional metrics about DS read operations on the selected DC which are gathered when the Directory Services Reads collection group is enabled.
Data displayed	<p>Directory Service Reads DRA, KCC, LSA and NSPI. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DRA. The percentage of directory reads coming from the Directory Replication Agent (DRA).• KCC. The percentage of directory reads coming from the Knowledge Consistency Checker (KCC).• LSA. The percentage of directory reads coming from the Local Security Authority (LSA).• NSPI. The percentage of directory reads coming from the Name Service Provider Interface (NSPI). <p>Directory Service Reads NTDSAPI, SAM and Other. This graph charts the following metrics:</p> <ul style="list-style-type: none">• NTDSAPI. The percentage of directory reads coming from Name Service Directory API (NTDSAPI) calls.• SAM. The percentage of directory reads coming from the Security Authentication Server (SAM).• Other. The percentage of directory reads coming from other components on the directory.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Directory Services Searches view

To display this view, enable the **Directory Services Searches Group** in the Directory Services section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Directory Services navigation tab for the selected DC in the Active Directory Explorer dashboard.

Table 36. Directory Services Searches view

Description	This view displays additional metrics about DS search operations on the selected DC which are gathered when the Directory Services Searches collection group is enabled.
Data displayed	<p>Directory Service Searches DRA, KCC, LDAP and LSA. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DRA. The percentage of directory searches performed by DRA.• KCC. The percentage of directory searches performed by KCC.• LDAP. The percentage of directory searches performed by Lightweight Directory Access Protocol (LDAP).• LSA. The percentage of directory searches performed by LSA.

Table 36. Directory Services Searches view

<p>Directory Service Searches NSPI, NTDSAPI, SAM and Other. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • NSPI. The percentage of directory searches performed by NSPI. • NTDSAPI. The percentage of directory searches performed by NTDSAPI calls. • SAM. The percentage of directory searches performed by SAM. • Other. The percentage of directory searches performed by other components on the directory. 	
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Directory Services Writes view

To display this view, enable the **Directory Services Writes Group** in the Directory Services section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Directory Services navigation tab for the selected DC in the Active Directory Explorer dashboard.

Table 37. Directory Services Writes view

Description	<p>This view displays additional metrics about DS write operations on the selected DC which are gathered when the Directory Services Writes collection group is enabled.</p>
Data displayed	<p>Directory Service Writes DRA, KCC and LDAP. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • DRA. The percentage of directory writes coming from DRA. • KCC. The percentage of directory writes coming from KCC. • LDAP. The percentage of directory writes coming from LDAP. <p>DS % Writes from LSA. This counter shows the percentage of directory writes coming from LSA.</p> <p>DS % Writes from NSPI. This counter shows the percentage of directory writes coming from NSPI.</p> <p>DS % Writes from NTDSAPI. This counter shows the percentage of directory writes coming from NTDSAPI.</p> <p>DS % Writes from SAM. This counter shows the percentage of directory writes coming from SAM.</p> <p>DS % Writes from Other. This counter shows the percentage of directory writes coming from other components in the directory.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Domain Controller Details view

This embedded view is part of the Site Environment Summary for an individual site in the Active Directory Environment dashboard.

Table 38. Domain Controller Details view

Description	This view lists the domain controllers that reside in the selected site. It provides the following details about the DCs in the selected site.
Data displayed	<ul style="list-style-type: none"> • State. Indicates the highest alarm triggered for each DC. • Name. Displays the name of each DC. • Roles. Displays the operations master roles 'owned' by the server: <ul style="list-style-type: none"> • Infrastructure Master - indicates that the DC is running the inter-domain daemon process that resolves references to objects in other domains that have been moved or renamed. • PDC Master - indicates that the DC can act as the PDC for down level backup domain controllers (BDCs) and clients. • RID Master - indicates that the DC can allocate RID pools to other DCs. • Multiple FMSO - indicates that the server 'owns' more than one operations master role. (Hovering your cursor over the Multiple FMSO entry displays a list of the roles owned by the server.) • n/a - indicates that the server does not 'own' any operations master roles. • Bytes In. Displays the rate at which bytes are received by the server. • Bytes Out. Displays the rate at which bytes are sent from the server.
Where to go next	Drill down on: <ul style="list-style-type: none"> • Domain Controller row. Displays the Domain Controller Explorer Summary view for the selected DC.

Domain Controllers view

To display this view, open the **Summary** navigation tab for an individual forest, domain or site in the Active Directory Explorer dashboard.

Table 39. Domain Controllers view

Description	This sortable list contains the following information for each DC in the selected forest, domain or site.
Data displayed	<ul style="list-style-type: none"> • State. Indicates the highest alarm triggered for each DC. • Name. Displays the name of each DC. • IP Address. Displays the IP address of each DC. • Purpose. Displays the purpose for this DC (e.g., Global Catalog, Domain Controller). • Roles. Displays the operations master role 'owned' by the server: <ul style="list-style-type: none"> • Infrastructure Master - indicates that the DC is running the inter-domain daemon process that resolves references to objects in other domains that have been moved or renamed. • PDC Master - indicates that the DC can act as the PDC for down level backup domain controllers (BDCs) and clients. • RID Master - indicates that the DC can allocate RID pools to other DCs. • Multiple FMSO - indicates that the server 'owns' more than one operations master role. • n/a - indicates that the server does not 'own' any operations master roles. • CPU. Displays the current CPU utilization on the server.

Table 39. Domain Controllers view

	<ul style="list-style-type: none"> • Memory. Displays the current memory utilization on the server.
	<ul style="list-style-type: none"> • Bytes In. Displays the rate at which bytes are received by the server.
	<ul style="list-style-type: none"> • Bytes Out. Displays the rate at which bytes are sent from the server.
	<ul style="list-style-type: none"> • Replication. Indicates whether replication for the selected DC is working properly.
	<ul style="list-style-type: none"> • Operating System. Displays the Windows® operating system running on the server.
Where to go next	Drill down on: <ul style="list-style-type: none"> • Domain Controller. Displays the Domain Controller Explorer Summary view for the selected DC.

FileReplicaConn Authentications/Bindings view

To display this view, enable the **FileReplicaConn Authentications/Bindings Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 40. FileReplicaConn Authentications/Bindings view

Description	This view displays authentication and binding metrics for the FileReplicaConn object in the selected DC which are gathered when the FileReplicaConn Authentications/Bindings collection group is enabled.
Data displayed	<p>Authentications and Bindings. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Authentications. Shows the number of authentications performed. • Bindings. Shows the number of bindings completed. <p>Authentications and Bindings in Error. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Authentications in Error. Shows the number of authentications performed in error. • Bindings in Error. Shows the number of bindings completed in error. <p>Communication Timeouts. This counter shows the number of communications that timed out.</p>
Where to go next	Drill down on: <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FileReplicaConn Change Orders view

To display this view, enable the **FileReplicaConn Change Orders Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 41. FileReplicaConn Change Orders view

Description	This view displays change order metrics for the FileReplicaConn object in the selected DC which are gathered when the FileReplicaConn Change Orders collection group is enabled.
Data displayed	<p>Local Change Orders. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Local Change Orders Sent. Shows the number of local change orders sent. • Local Change Orders Sent at Join. Shows the number of local change orders sent at Join. • Outbound Change Orders Dampened. Shows the number of outbound change orders dampened. <p>Packets Sent. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Packets Sent. Shows the number of packets sent. • Packets Sent in Bytes. Shows the number of packets (in bytes) sent. • Packets Sent in Error. Shows the number of packets sent in error. <p>Remote Change Orders. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Remote Change Orders Received. Shows the number of remote change orders received. • Remote Change Orders Sent. Shows the number of remote change orders sent. <p>Unjoins. This graph charts the number of unjoin operations being performed. It provides a comparison against the computed average for the specified time interval.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FileReplicaConn Fetch view

To display this view, enable the **FileReplicaConn Fetch Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 42. FileReplicaConn Fetch view

Description	This view displays fetch metrics for the FileReplicaConn object in the selected DC which are gathered when the FileReplicaConn Fetch collection group is enabled.
Data displayed	<p>Fetch Requests. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Fetch Requests Received. Shows the number of fetch requests that have been received. • Fetch Requests Sent. Shows the number of fetch requests that have been sent. <p>Join Notifications Received. This counter shows the number of join notifications that have been received.</p> <p>Join Notifications Sent. This counter shows the number of join notifications that have been sent.</p> <p>Fetch Blocks Received. This counter shows the number of fetch blocks that have been received.</p>

Table 42. FileReplicaConn Fetch view

	Fetch Blocks Sent. This counter shows the number of fetch blocks that have been sent.
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FileReplicaSet Authentications/Bindings view

To display this view, enable the **FileReplicaSet Authentications/Bindings Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 43. FileReplicaSet Authentications/Bindings view

Description	This view displays authentication and binding metrics for the FileReplicaSet object in the selected DC which are gathered when the FileReplicaSet Authentications/Bindings collection group is enabled.
Data displayed	<p>Authentications and Bindings. This graph charts the following metrics:</p> <ul style="list-style-type: none"> Authentications. Shows the number of authentications performed. Bindings. Shows the number of bindings completed. <p>Authentications and Bindings in Error. This graph charts the following metrics:</p> <ul style="list-style-type: none"> Authentications in Error. Shows the number of authentications performed in error. Bindings in Error. Shows the number of bindings completed in error.
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FileReplicaSet Change Orders view

To display this view, enable the **FileReplicaSet Change Orders Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 44. FileReplicaSet Change Orders view

Description	This view displays change order metrics for the FileReplicaSet object in the selected DC which are gathered when the FileReplicaSet Change Orders collection group is enabled.
Data displayed	<p>Change Orders. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Change Orders Aborted. Shows the number of change orders that were aborted. • Change Orders Evaporated. Shows the number of change orders that evaporated. • Change Orders Issued. Shows the number of change orders that were issued. • Change Orders Morphed. Shows the number of change orders morphed. • Change Orders Propagated. Shows the number of change order propagated. <p>Change Orders Retried. This counter shows the number of change orders that were retried.</p> <p>Change Orders Retried at Fetch. This counter shows the number of change orders that were retried at fetch.</p> <p>Change Orders Retried at Generate. This counter shows the number of change orders that were retried at generate.</p> <p>Change Orders Retried at Install. This counter shows the number of change orders that were retried at install.</p> <p>Change Orders Retried at Rename. This counter shows the number of change orders that were retried at rename.</p> <p>Change Orders Retired. This graph charts the number of change orders that were retired.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FileReplicaSet DS Communications view

To display this view, enable the **FileReplicaSet DS Communications Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 45. FileReplicaSet DS Communications view

Description	This view displays DS communication metrics for the FileReplicaSet object in the selected DC which are gathered when the FileReplicaSet DS Communications collection group is enabled.
Data displayed	<p>DS Bindings. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • DS Bindings. Shows the number of directory service bindings. • DS Bindings in Error. Shows the number of directory service bindings that were in error. <p>DS Objects. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • DS Objects. Shows the number of directory objects. • DS Objects in Error. Shows the number of directory objects that were in error.

Table 45. FileReplicaSet DS Communications view

	<p>DS Polls. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DS Polls. Shows the number of directory service polls.• DS Polls with Changes. Shows the number of directory service polls with changes.• DS Polls without Changes. Shows the number of directory service polls without changes.
	<p>Communication Timeouts. This graph charts the number of communications that timed out. It provides a comparison against the computed average for the specified time interval.</p>
	<p>DS Searches. This graph charts the following metrics:</p> <ul style="list-style-type: none">• DS Searches. Shows the number of directory service searches.• DS Searches in Error. Shows the number of directory service searches that were in error.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FileReplicaSet Files view

To display this view, enable the **FileReplicaSet Files Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 46. FileReplicaSet Files view

Description	This view displays metrics for FileReplicaSet files in the selected DC which are gathered when the FileReplicaSet Files collection group is enabled.
Data displayed	<p>Bytes of Files Installed. This graph charts the number of bytes of files installed.</p> <p>Bytes of Staging. This graph charts the following metrics relating to staging which is the temporary storage of files prior to replication:</p> <ul style="list-style-type: none">• Bytes of Staging Fetched. Shows the number of bytes of staging that were fetched.• Bytes of Staging Generated. Shows the number of bytes of staging that were generated.• Bytes of Staging Regenerated. Shows the number of bytes of staging that were regenerated.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FileReplicaSet Local Change Orders view

To display this view, enable the **FileReplicaSet Local Change Orders Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 47. FileReplicaSet Local Change Orders view

Description	This view displays local change order metrics for the FileReplicaSet object in the selected DC which are gathered when the FileReplicaSet Local Change Orders collection group is enabled.
Data displayed	<p>Local Change Orders. This graph charts the following metrics:</p> <ul style="list-style-type: none">• Local Change Orders Aborted. Shows the number of local change orders that were aborted.• Local Change Orders Issued. Shows the number of local change orders that were issued.• Local Change Orders Morphed. Shows the number of local change orders that were morphed.• Local Change Orders Propagated. Shows the number of local change order that were propagated. <p>Local Change Orders Retried. This counter shows the number of local change orders that were retried.</p> <p>Local Change Orders Retried at Fetch. This counter shows the number of local change orders that were retried at fetch.</p> <p>Local Change Orders Retried at Generate. This counter shows the number of local change orders that were retried at generate.</p> <p>Local Change Orders Retried at Install. This counter shows the number of local change orders that were retried at install.</p> <p>Local Change Orders Retried at Rename. This counter shows the number of local change orders that were retried at rename.</p> <p>Local Change Orders Retired. This graph charts the number of local change orders that were retired.</p> <p>Local Change Orders Sent. This graph charts the following metrics:</p> <ul style="list-style-type: none">• Local Change Orders Sent. Shows the number of local change orders that were sent.• Local Change Orders Sent at Join. Shows the number of local change orders that were sent at join. <p>Change Orders Dampened. This graph charts the following metrics:</p> <ul style="list-style-type: none">• Outbound Change Orders Dampened. Shows the number of outbound change orders that were dampened.• Inbound Change Orders Dampened. Shows the number of inbound change orders that were dampened.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FileReplicaSet Packets view

To display this view, enable the **FileReplicaSet Packets Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 48. FileReplicaSet Packets view

Description	This view displays packet metrics for the FileReplicaSet object in the selected DC which are gathered when the FileReplicaSet Packets collection group is enabled.
Data displayed	<p>Packets in Bytes. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Packets Received in Bytes. Shows the number of packets (in bytes) that were received. • Packets Sent in Bytes. Shows the number of packets (in bytes) that were sent. <p>Packets in Error. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Packets Received in Error. Shows the number of packets that were received in error. • Packets Sent in Error. Shows the number of packets that were sent in error.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FileReplicaSet Remote Change Orders view

To display this view, enable the **FileReplicaSet Remote Change Orders Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

i | **NOTE:** Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 49. FileReplicaSet Remote Change Orders view

Description	This view displays remote change order metrics for the FileReplicaSet object in the selected DC which are gathered when the FileReplicaSet Remote Change Orders collection group is enabled.
Data displayed	<p>Remote Change Orders. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Remote Change Orders Aborted. Shows the number of remote change orders that were aborted. • Remote Change Orders Issued. Shows the number of remote change orders that were issued. • Remote Change Orders Morphed. Shows the number of remote change orders that were morphed. • Remote Change Orders Propagated. Shows the number of remote change orders that were propagated. • Remote Change Orders Received. Shows the number of remote change orders that were received. <p>Remote Change Orders Retried. This counter shows the number of remote change orders that were retried.</p> <p>Remote Change Orders Retried at Fetch. This counter shows the number of remote change orders that were retried at fetch.</p> <p>Remote Change Orders Retried at Generate. This counter shows the number of remote change orders that were retried at generate.</p> <p>Remote Change Orders Retried at Install. This counter shows the number of remote change orders that were retried at install.</p> <p>Remote Change Orders Retried at Rename. This counter shows the number of remote change orders that were retried at rename.</p>

Table 49. FileReplicaSet Remote Change Orders view

	Remote Change Orders Retired. This graph charts the number of remote change orders that were retired. It provides a comparison against the computed average for the specified time interval.
	Remote Change Orders Sent. This graph charts the number of remote change orders that were sent. It provides a comparison against the computed average for the specified time interval.
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FRS Performance Health view

To display this embedded view, select the **FRS** navigation tab for an individual DC in the Active Directory Explorer dashboard.

NOTE: Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 50. FRS Performance Health view

Description	This view displays the file replication service (FRS) performance metrics for the selected DC. These counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	<p>FRS Percent Memory. This graph charts the percent of memory being consumed by the NTFRS process on the selected DC over the specified time interval.</p> <p>FRS Percent CPU. This graph charts the percent of CPU being consumed by the NTFRS process on the selected DC. It provides a comparison against the computed average for the specified time interval.</p> <p>FRS Working Set. This graph charts the number of memory pages recently used by the threads in the NTFRS process on the selected DC. It provides a comparison against the computed average for the specified time interval.</p> <p>Change Orders Received and Sent. This graph charts the following metrics:</p> <ul style="list-style-type: none"> Change Orders Received. Shows the number of change orders that were received. Change Orders Sent. Shows the number of change orders that were sent. <p>Packets Received and Sent. This graph charts the following metrics:</p> <ul style="list-style-type: none"> Packets Received. Shows the number of packets that were received. Packets Sent. Shows the number of packets that were sent. <p>KB of Staging Space Free. This button displays the amount of free staging space, in kilobytes, on the selected DC.</p> <p>KB of Staging Space. This graph charts the number of kilobytes of staging space that are in use. It provides a comparison against the computed average for the specified time interval.</p> <p>Files Installed. This graph charts the total number of file installed. It provides a comparison against the computed average for the specified time interval.</p> <p>USN Records Accepted. This graph charts the number of times NTFS change log records have been accepted for replication. It provides a comparison against the computed average for the specified time interval.</p>
Where to go next	Drill down on:

Table 50. FRS Performance Health view

- **FRS Performance Health title** - displays an Alarms popup listing the current FRS alarms that are outstanding for the selected DC.
- Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FRS Replica Sets view

To display this view, enable the **FRS Replica Sets Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

NOTE: Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 51. FRS Replica Sets view

Description	This view displays metrics related to file replica sets in the selected DC which are gathered when the FRS Replica Sets collection group is enabled.
Data displayed	<p>Replica Sets. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Replica Sets Created. Shows the number of replica sets that were created. • Replica Sets Deleted. Shows the number of replica sets that were deleted. • Replica Sets Removed. Shows the number of replica sets that were removed. • Replica Sets Started. Shows the number of replica sets that were started.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FRS Staging Files view

To display this view, enable the **FRS Staging Files Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab in the Active Directory Explorer dashboard.

NOTE: Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 52. FRS Staging Files view

Description	This view displays metrics related to FRS staging files in the selected DC which are gathered when the FRS Staging Files collection group is enabled.
Data displayed	<p>Staging Files. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Staging Files Fetched. Shows the number of staging files that were fetched. • Staging Files Generated. Shows the number of staging files that were generated. • Staging Files Generated with Error. Shows the number of staging files that were generated with errors. • Staging Files Regenerated. Shows the number of staging files that were regenerated.

Table 52. FRS Staging Files view

	<p>Files Installed with Errors. This graph charts the number of files that were installed with error.</p>
	<p>Fetch Blocks Received and Sent. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Fetch Blocks Received. Shows the number of fetch blocks that were received. • Fetch Blocks Sent. Shows the number of fetch blocks that were sent.
	<p>Fetch Blocks in Bytes. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Fetch Blocks Received in Bytes. Shows the number of fetch blocks (in bytes) that were received. • Fetch Blocks Sent in Bytes. Shows the number of fetch blocks (in bytes) that were sent.
	<p>Fetch Requests. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • Fetch Requests Received. Shows the number of fetch requests that were received. • Fetch Requests Sent. Shows the number of fetch requests that were sent.
	<p>Join Notifications Received. This counter shows the number of join notifications that were received during the selected time interval.</p>
	<p>Join Notifications Sent. This counter shows the number of join notifications that were sent during the selected time interval.</p>
	<p>Threads Exited. This counter shows the number of threads that were exited during the selected time interval.</p>
	<p>Threads Started. This counter shows the number of threads that were started during the selected time interval.</p>
	<p>Joins. This counters shows the number of join operations performed during the selected time interval.</p>
	<p>Unjoins. This counter shows the number of unjoin operations performed during the selected time interval.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

FSMO Roles view (Domain)

This embedded view is part of the Domain Environment Summary for an individual domain in the Active Directory Environment dashboard.

Table 53. FSMO Roles view (Domain)

Description	This view contains a list of the operations master roles 'owned' by DCs in the selected domain.
Data displayed	<ul style="list-style-type: none"> • State. For each operations master role listed, this field indicates the current state of the DC that 'owns' the role. • Role. Lists the operations master roles 'owned' by DCs in the selected domain. • Name. For each operations master role listed, this field displays the name of the DC that 'owns' the operations master role.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Domain Controller. Displays the Domain Controller Explorer Summary view for the selected DC.

FSMO Roles view (Forest)

This embedded view is part of the Forest Environment Summary for an individual forest in the Active Directory Environment dashboard.

Table 54. FSMO Roles view (Forest)

Description	This view contains the following information for the forest level operations master roles 'owned' by DCs in the selected forest.
Data displayed	<ul style="list-style-type: none">• Domain. For each operations master role listed, this field displays the name of the domain where the DC that 'owns' the operations master role resides.• Server. For each operations master role listed, this field displays the name of the DC that 'owns' the operations master role.
Where to go next	Clicking a server in this view displays an Alarms popup listing the current alarms that are outstanding for the selected server.

Host Monitor view

This embedded view is part of the Domain Controller Environment Summary for an individual DC in the Active Directory Environment dashboard.

i **NOTE:** When the host machine is a virtual machine that is being monitored by Foglight for VMWare or Foglight for Hyper-V, this view is replaced with two views: one that displays the name of the virtual machine and one that displays the name of the host server.

Table 55. Host Monitor view

Description	This view displays the name of the target server from which data is being collected.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Host Monitor Name. Displays the Host Monitor dashboard that provides a real-time overview of how a host is performing. For more information about the Host Monitor dashboard, see the <i>Foglight User Guide</i> or online help. <p>NOTE: When the host is a virtual machine that is being monitored by Foglight for VMWare or Foglight for Hyper-V, this link drills down to the Explorer Summary page for the selected DC. There is also an additional link that drills down to the metrics for the host of the virtual machine. Both of these drill down views are part of Foglight for VMWare or Foglight for Hyper-V.</p>

Inter-Site Transports view

This embedded view is part of the Site Environment Summary for an individual site in the Active Directory Environment dashboard.

Table 56. Inter-Site Transports view

Description	This sortable list contains the following information for each site link in the selected site.
Data displayed	<ul style="list-style-type: none">• Name. Displays the name of the site link.• Type. Displays the type of link.• Description. If available, displays the description of the site link.• Cost. Displays the relative cost of replication using the link.

Table 56. Inter-Site Transports view

	<ul style="list-style-type: none"> • Replication Interval. Displays the replication frequency (number of minutes between replications).
Where to go next	N/A

Inventory By Category view

This embedded view is part of the Forest Environment Summary, Domain Environment Summary and Site Environment Summary, which is displayed when an individual forest, domain or site is selected in the Object Tree view (Quick View) on the Active Directory Environment dashboard.

Table 57. Inventory By Category view

Description	This view displays the number of servers performing different tasks for the selected forest, domain or site and the number of those servers in each alarm state.
Data displayed	<p>For a forest object, the following is displayed:</p> <ul style="list-style-type: none"> • FSMO Holders. Indicates how many servers in this forest are operation masters and the alarm state for each of these servers. • DNS Servers. Indicates how many DNS servers reside in this forest and the alarm state for each of these servers. • Global Catalogs. Indicates how many servers in this forest are hosting a Global Catalog and the alarm state for each of these servers. <p>For a domain object, the following is displayed:</p> <ul style="list-style-type: none"> • Sub Domains. Indicates how many subordinate domains are in this domain and the alarm state for each of these sub domains. • DNS Servers. Indicates how many DNS servers reside in this domain and the alarm state for each of these servers. • FSMO Holders. Indicates how many servers in this domain are operations masters and the alarm state for each of these servers. • Global Catalogs. Indicates how many servers in this domain are hosting a Global Catalog and the alarm state for each of these servers. <p>For a site object, the following is displayed:</p> <ul style="list-style-type: none"> • Domains. Indicates how many domains reside in this site and the alarm state for each domain. • DNS Servers. Indicates how many DNS servers reside in this site and the alarm state for each of these servers. • FSMO Holders. Indicates how many servers in this site are operation masters and the alarm state for each of these servers.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Category Heading. Displays an Inventory popup that displays the names of the servers performing the selected task. • Domain Controller Inventory Popup - Domain Controller. Displays the Domain Controller Explorer Summary view for the selected DC. • Alarm Icon or Number. Displays an Alarms popup that displays the current alarms for the DCs performing the selected task. • Alarms Popup - Domain Controller. Allows you to display the metrics for the selected DC in either the Active Directory Explorer or Quick View. • Alarms Popup - AD object icon, Severity icon, Time, or Alarm Message. Displays an Alarm Details popup containing details about the selected alarm. • Alarms Popup - Info icon. Displays a metrics popup containing a trend graph, metric description and troubleshooting tips for the selected alarm.

NOTE: The popup trend graph is scoped to the time when the alarm was triggered.

IP Subnets view

This embedded view is part of the Site Environment Summary for an individual site in the Active Directory Environment dashboard.

Table 58. IP Subnets view

Description	This view lists the IP subnets associated with the selected site.
Where to go next	N/A

Key Distribution Center view

To display this view, enable the **Key Distribution Center Group** in the Directory Services section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Directory Services navigation tab in the Active Directory Explorer dashboard.

Table 59. Key Distribution Center view

Description	This view displays additional Key Distribution Center (KDC) metrics for the selected DC which are gathered when the Key Distribution Center collection group is enabled.
Data displayed	Requests. This graph charts the following metrics: <ul style="list-style-type: none">• KDC AS Requests. Shows the number of Authentication Server (AS) requests serviced by the KDC per second.• KDC TGS Requests. Shows the number of Ticket Granting Service (TGS) requests serviced by the KDC per second.
	NTLM Authentications. This graph charts the number of NTLM authentications serviced by the selected DC per second.
Where to go next	Drill down on: <ul style="list-style-type: none">• Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

LDAP view

To display this view, enable the **LDAP Group** in the Directory Services section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Directory Services navigation tab in the Active Directory Explorer dashboard.

Table 60. LDAP view

Description	This view displays additional LDAP metrics for the selected DC which are gathered when the LDAP collection group is enabled.
Data displayed	LDAP Active Threads. This graph charts the current number of threads in used by the LDAP subsystem of the local directory service. It provides a comparison against the computed average for the specified time interval.
	LDAP Connections/sec. This graph charts the following metrics: <ul style="list-style-type: none">• LDAP Closed Connections/sec. Shows the number of LDAP connections that have been closed in the last second.• LDAP New Connections/sec. Shows the number of new LDAP connections that have arrived in the last second.• LDAP New SSL Connections/sec. Shows the number of new SSL or TLS connections that arrived in the last second.

Table 60. LDAP view

	LDAP Successful Binds/sec. This graph charts the number of LDAP binds being performed per second. It provides a comparison against the computed average for the specified time interval.
	LDAP UDP Operations/sec. This graph charts the number of UDP operations the LDAP service is processing per second. It provides a comparison against the computed average for the specified time interval.
	LDAP Writes/sec. This graph charts the rate at which LDAP clients perform write operations per second. It provides a comparison against the computed average for the specified time interval.
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Memory view

This embedded view is part of the Resource Utilization Details view. To display this view, select the **Resource Utilization** title or **Details** link (upper right corner) at the top of the Resource Utilization view for an individual DC in the Active Directory Explorer dashboard.

Table 61. Memory view

Description	This view displays memory utilization metrics for the selected DC. The counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	Available Bytes. Displays the amount of memory (in MB) available.
	Committed Bytes. Displays the percent of total bytes committed.
	Memory Available and Consumed. This graph charts the following metrics over the specified time interval: <ul style="list-style-type: none"> Memory Capacity. Shows the maximum or minimum amount of memory a computer or hardware device is capable of having. Memory Consumed. Shows the amount of memory being used.
	Page Rate/sec. The counter displays the rate at which pages are currently being read from or written to memory in order to resolve hard page faults.
	Memory Pages/sec. This graph charts the rate at which pages are read from or written to memory in order to resolve hard page faults for the specified time interval.
	Memory Cache Bytes. This graph charts the size of the file system cache. It provides a comparison against the computed average for the specified time interval.
	Memory Pool Paged and Non Paged Bytes. This graph charts the following metrics over the specified time interval: <ul style="list-style-type: none"> Memory\Pool Paged Bytes. Shows the portion of shared system memory that can be paged to the disk paging file. Memory\Pool Non Paged Bytes. Shows the portion of physical memory that can be accessed from any address space without incurring paging I/O.
	.NET® CLR Exceptions Thrown/sec. This graph charts the number of exceptions thrown per second during the specified time interval. It provides a comparison against the defined warning, critical and fatal levels.
	.NET CLR Percent Time in Garbage Collection. This graph charts the percentage of time being spent performing garbage collections during the specified time interval. It provides a comparison against the defined warning, critical and fatal levels.

Table 61. Memory view

.NET CLR Memory Bytes in All Heaps. This graph charts the memory usage by all managed resources during the specified time interval. It provides a comparison against the computed average for the specified time interval.	
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Network view

This embedded view is part of the Resource Utilization Details view. To display this view, select the **Resource Utilization** title or **Details** link (upper right corner) at the top of the Resource Utilization view for an individual DC in the Active Directory Explorer dashboard.

Table 62. Network view

Description	This view displays network utilization metrics for the selected DC. The counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	<p>Network Interface. Displays a list of network interfaces available on the selected DC. Selecting a network interface in this view displays the following metrics for the selected interface.</p> <ul style="list-style-type: none"> Available Bandwidth. This counter displays the current percentage of bandwidth that is available. Bandwidth. This graph charts the network bandwidth (MB/sec) for the selected network interface. It provides a comparison against the computed average for the specified time interval. Output Queue Length. This graph charts the length of the output queue over. It provides a comparison against the computed average for the specified time interval. Send & Receive Rates. These pulse gauges display the rate at which data is sent and received over the selected network interface. Packet Outbound Errors. This graph charts the number of outbound packets that could not be transmitted due to errors. It provides a comparison against the defined fatal, critical and warning levels.
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Processor view

This embedded view is part of the Resource Utilization Details view. To display this view, select the **Resource Utilization** title or **Details** link (upper right corner) at the top of the Resource Utilization view for an individual DC in the Active Directory Explorer dashboard.

Table 63. Processor view

Description	This view displays processor utilization metrics for the selected DC. The counters and indicators in this view change color based on overall consumption or deviation from normal levels.
Data displayed	<p>System\Processor Queue Length. This button indicates the number of threads each processor is currently servicing. This number should not be greater than five per processor.</p> <p>Processor Queue Length can be used to identify when processor contention or high CPU utilization is caused by the processor capacity being insufficient to handle the assigned workload.</p> <p>Percent Processor Time. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> • % User Time. Shows the percentage of time that is spent in user mode. User mode is a restricted processing mode designed for applications, environment subsystems, and integral subsystems. • % Privileged Time. Shows the percentage of time that is spent in privileged mode. Privilege mode is a processing mode designed for operating system components and hardware-manipulating drivers. It allows direct access to hardware and memory. • % Processor Time. Shows the percentage of time that the processor is executing application or operation system processes.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Replication Performance Health view

To display this embedded view, select the **Replication** navigation tab for an individual DC in the Active Directory Explorer dashboard.

Table 64. Replication Performance Health view

Description	This view displays replication performance metrics for the selected DC. The counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	<p>Replication Failures. This table displays the following information about replication failures that have occurred during the specified time interval:</p> <ul style="list-style-type: none"> • Time • Partition • Reason Code • Reason <p>Replication Queue Length. The button displays the current length of the replication queue. The graph charts the length of the replication queue over the specified time interval. It provides a comparison against the computed average.</p> <p>Replication Requests. This counter displays the rate at which replication requests are being made.</p> <p>Replication Requests/sec. This graph charts the number of replication requests made per second. It provides a comparison against the computed average for the specified time interval.</p>

Table 64. Replication Performance Health view

	<p>DRA Pending Replication Synchronizations. This graph charts the number of directory synchronizations that are queued for this server awaiting to be processed. It provides a comparison against the computed average for the specified time interval.</p>
	<p>DRA Inbound and Outbound Values Total/sec. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> • DRA Inbound Values Total/sec. Shows the total number of object property values received from inbound replication partners. Each inbound object has one or more properties, and each property has zero or more values. Zero values indicate property removal. • DRA Outbound Values Total/sec. Shows the number of object property values sent to outbound replication partners.
	<p>DRA Objects Filtered and Applied/sec. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> • DRA Inbound Objects Applied/sec. Shows the rate at which replication updates that are received from replication partners are applied by the local directory service. This count excludes changes that are received but not applied (for example, when a change is already present). • DRA Inbound Objects Filtered/sec. Shows the number of objects received from inbound replication partners that contained no updates that needed to be applied. • DRA Outbound Objects Filtered/sec. Shows the number of objects looked at by outbound replication partners that were determined to contain no updates that the needed to be applied by the outbound partner.
	<p>DRA Inbound Object Updates Remaining in Packet. This graph charts the number of object updates received in the current directory replication update packet that have not been applied to the local server. It provides a comparison against the computed average for the specified time interval.</p>
	<p>DRA Objects In/Out. These pulse gauges indicate the rate at which objects are being replicated.</p>
	<p>DRA Bytes In/Out. These pulse gauges indicate the rate at which bytes of data are being replicated.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Resource Utilization view

To display this view, select the **Summary** navigation tab for an individual DC in the Active Directory Explorer dashboard. This view is located at the top of the Primary view.

Table 65. Resource Utilization view

Description	This view displays the resource utilization metrics associated with the selected DC over the specified time interval. The counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	<p>CPU Load. This counter indicates the total CPU load per second for the selected DC.</p> <p>CPU Utilization. This graph charts CPU utilization for the selected DC over the specified time interval. It provides a comparison against the defined warning, critical and fatal alarm levels.</p> <p>Network I/O. This counter displays the rate at which data is coming in and going out over the network interface on the selected DC.</p>

Table 65. Resource Utilization view

	<p>Network Utilization. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> • Send Rate. Displays how many bytes of data are being sent to the NIC each second. • Receive Rate. Displays how many bytes of data are coming in from the NIC each second.
	<p>Total Memory. This button displays the maximum capacity of memory on the selected DC.</p>
	<p>Memory In Use. This button displays the actual amount of physical memory currently being used.</p>
	<p>Memory Utilization. This graph charts the memory utilization for the selected DC. It provides a comparison between consumed memory and the computed average for the specified time interval.</p>
	<p>Disk I/O. This counter displays the rate at which the disk I/O system on the selected DC is processing disk reads and writes.</p>
	<p>Disk Utilization. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> • Read Rate. Displays the rate at which data is being read by the disk. • Write Rate. Displays the rate at which data is being written to the disk.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Resource Utilization title. Displays the Resource Utilization Details view for the selected DC • Details link. Displays the Resource Utilization Details view for the selected DC. • Clicking a counter in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Security Accounts Manager view

To display this view, enable the **Security Accounts Manager Group** in the Directory Services section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the Directory Services navigation tab in the Active Directory Explorer dashboard.

Table 66. Security Accounts Manager view

Description	<p>This view displays additional Security Accounts Manager (SAM) metrics for the selected DC which are gathered when the Security Accounts Manager collection group is enabled.</p>
Data displayed	<p>SAM Creations/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • SAM Machine Creation Attempts/sec. Shows the number of create computer account attempts are being made per second. • SAM Successful Computer Creations/sec. Shows the number of times a computer account was successfully created per second. • SAM Successful User Creations/sec. Shows the number of times a user account was successfully created per second. • SAM User Creation Attempts/sec. Shows the number of create user account attempts are being made per second.

Table 66. Security Accounts Manager view

	<p>SAM Changes/sec. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • SAM Membership Changes/sec. Shows the number of group membership changes being performed per second, across all global, universal and nested groups. • SAM Password Changes/sec. Shows the number of SAM password changes being performed per second.
	<p>SAM Evaluation Latencies. This graph charts the following metrics:</p> <ul style="list-style-type: none"> • SAM Account Group Evaluation Latency. Shows the mean latency of the last 100 account and universal group evaluations performed for authentication. • SAM Resource Group Evaluation Latency. Shows the mean latency of the last 100 resource group evaluations performed for authentication.
	<p>SAM Display Information Queries/sec. This graph charts the number of queries being performed per second to obtain display information.</p>
	<p>SAM Enumerations/sec. This graph charts the net user, net group, and net local function enumerations being performed per second.</p>
	<p>SAM Global and Universal Membership Evaluations/sec. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> • SAM Global Group Membership Evaluations/sec. Shows the number of domain global group membership evaluations being performed per second at authentication time. • SAM Universal Group Membership Evaluations/sec. Shows the number of universal group membership evaluations being performed per second at authentication time.
	<p>SAM Domain Local Group Membership Evaluations/sec. This counter shows the number of domain local group membership evaluations being performed per second at authentication time.</p>
	<p>SAM GC Evaluations/sec. This counter shows the number of universal group membership evaluations that are being performed per second on a global catalog DC from non-global catalog DCs.</p>
	<p>SAM Non-Transitive Membership Evaluations/sec. This counter shows the number of new user and local groups encountered per second when performing a non-transitive membership evaluation.</p>
	<p>SAM Transitive Membership Evaluations/sec. This counter shows the number of new groups encountered per second when performing a transitive membership evaluation.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Server Health view

This embedded view is part of the Domain Controller Environment Summary when an individual DC is selected in the Object Tree view (Quick View) in the Active Directory Environment dashboard.

Table 67. Server Health view

Description	This view summarizes the current health of the selected DC. These counters change colors based on overall consumption or deviation from normal levels.
Data displayed	<p>CPU. This counter displays what percent of the CPU is currently being used.</p> <p>Memory. This counter displays what percent of memory is currently being used. It can be used to determine whether you have memory problems.</p>

Table 67. Server Health view

	Network. This counter indicates the rate at which data is currently being transferred through the network interface.
	Storage. This counter indicates the percent of disk space being used. It also displays the amount of free space still available.
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Statistics view

This embedded view is part of the Forest Environment Summary and Domain Environment Summary when an individual forest or domain is selected in the Object Tree view (Quick View) in the Active Directory Environment dashboard.

Table 68. Statistics view

Description	This view provides statistics regarding the Active Directory® accounts in the selected forest or domain.
Data displayed	<ul style="list-style-type: none"> Users. Indicates how many Active Directory user accounts are in the selected forest or domain. Groups. Indicates how many Active Directory group accounts are in the selected forest or domain. Computers. Indicates how many computer accounts are in the selected forest or domain.
Where to go next	N/A

Storage view

This embedded view is part of the Resource Utilization Details view. To display this view, select the **Resource Utilization** title or the **Details** link (upper right corner) at the top of the Resource Utilization view for an individual DC in the Active Directory Explorer dashboard.

Table 69. Storage view

Description	This view displays storage utilization metrics for the selected DC.
Data displayed	<p>Logical Disk Read and Write Time. The counters display the current average time for the following counters:</p> <ul style="list-style-type: none"> Avg. Disk Read. Shows the average time, in milliseconds, it takes to read data from the disk. Avg. Disk Write. Shows the current average time, in milliseconds, it takes to write data to the disk. <p>The graph charts the following counters over the specified time interval:</p> <ul style="list-style-type: none"> Avg. Read Time. Shows the average time, in seconds, it takes to read data from the disk. <p>Avg. Write Time. Shows the average time, in seconds, it takes to write data to the disk.</p>

Table 69. Storage view

	<p>Physical Disk Read and Write Time. The counters display the current average time for the following counters:</p> <ul style="list-style-type: none"> • Avg. Disk Read. Shows the average time, in milliseconds, it takes to read data from the disk. • Avg. Disk Write. Shows the current average time, in milliseconds, it takes to write data to the disk.
	<p>The graph charts the following counters over the specified time interval:</p> <ul style="list-style-type: none"> • Avg. Read Time. Shows the average time, in seconds, it takes to read data from the disk. <p>Avg. Write Time. Shows the average time, in seconds, it takes to write data to the disk.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Summary and Resource Information view

This embedded view is part of the Domain Explorer Summary view when an individual DC is selected in the Active Directory Enterprise view on the Active Directory Explorer dashboard.

Table 70. Summary and Resource Information view

Description	This view displays the following information about the selected DC:
Data displayed	<p>DC Name. Displays the name of the selected DC.</p> <p>IP Address. Displays the IP address of the selected DC.</p> <p>Operating System. Displays the operating system running on the selected DC.</p> <p>FQDN. Displays the fully-qualified domain name of the domain where the selected DC resides.</p> <p>Uptime. Displays how long the server has been up and running.</p> <p>Site. Displays the name of the site to which the selected DC belongs.</p> <p>Processors. Displays the number of CPUs on the selected DC.</p> <p>Memory Capacity. Displays the memory capacity of the selected DC.</p> <p>Network Interfaces. Displays the number of network interfaces available on the selected DC.</p> <p>Storage Devices. Displays the number of storage devices on the selected DC.</p>
Where to go next	N/A

Top AD Metrics view

The Top AD Metrics view is part of the Domain Controller Environment Summary when an individual DC is selected in the Object Tree view (Quick View) on the Active Directory Environment dashboard. The contents of this view depends on the heading selected at the top of the view.

i | **NOTE:** Click on the status indicator to the left of a heading to display an alarm popup listing the active alarms for the selected category.

Table 71. Top AD Metrics view - Database

Description	When Database is selected, this view displays the following metrics for the Active Directory® database on the selected DC. These counters and indicators change colors based on overall consumption or deviation from normal levels:
Data displayed	<p>NTDS.DIT Size. The metrics indicator shows the size of the Active Directory database and indicates the alarm level based on the predefined threshold. The graph charts the size (in MB) of the database over the specified time interval. It provides a comparison against the computed average.</p> <p>Bytes Read. This counter shows the rate at which file bytes are read from the database.</p> <p>Bytes Read/sec. This graph charts the rate at which file bytes are read from the database. It provides a comparison against the computed average for the specified time interval.</p> <p>Bytes Written. This counter shows the rate at which file bytes are written to the database.</p> <p>Bytes Written/sec. This graph charts the rate at which file bytes are written to the database. It provides a comparison against the computed average for the specified time interval.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Table 72. Top AD Metrics view - DFS-R

Description	When DFS-R is selected, this view display distributed file system (DFS) replication service metrics for the selected DC. These counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	<p>Total Files Received. This graph charts the number of files that were received by the replicated folder. It provides a comparison against the computed average for the specified time interval.</p> <p>Staging Space in Use. This graph charts the amount of staging space (in bytes) being used by the files and folders currently in the Staging folder. It provides a comparison against the computed average for the specified time interval.</p>
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Table 73. Top AD Metrics view - DS

Description	When DS is selected, this view displays directory service related metrics for the selected DC. The counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	<p>LDAP Bind Response Time. This button shows the amount of time it is took to complete the last LDAP bind request.</p> <p>LDAP Bind Time. This graph charts the amount of time it took to complete successful LDAP bind requests. It provides a comparison against the computed average for the specified time interval.</p> <p>DS Directory Reads. This counter shows the rate at which DS directory reads are taking place.</p>

Table 73. Top AD Metrics view - DS

	DS Directory Reads/sec. This graph charts the number of DS directory reads taking place per second. It provides a comparison against the computed average for the specified time interval.
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Table 74. Top AD Metrics view - FRS

Description	When FRS is selected, this view display file replication service metrics for the selected DC. These counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	<p>Change Orders Received and Sent. This graph charts the following metrics over the specified time interval:</p> <ul style="list-style-type: none"> Change Orders Received. Shows the number of change orders that were received. Change Orders Sent. Shows the number of change orders that were sent. <p>KB of Staging Space Free. This button displays the current amount of free staging space, in kilobytes.</p> <p>KB of Staging Space. This graph charts the amount of staging space being used. It provides a comparison against the computed average for the specified time interval.</p>
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Table 75. Top AD Metrics view - Replication

Description	When Replication is selected, this view display replication metrics for the selected DC. These counters and indicators change colors based on overall consumption or deviation from normal levels.
Data displayed	<p>Replication Failures. Displays the number of replication failures encountered during the specified time interval.</p> <p>DRA Objects In/Out. These pulse gauges show the rate at which data objects are replicated in and out of the selected DC.</p> <p>DRA Bytes In/Out. These pulse gauges show the rate at which data bytes are replicated in and out of the selected DC.</p> <p>Replication Requests. This counter displays the rate at which replication requests are being processed by the DC.</p> <p>Replication Requests/sec. This graph charts the number of replication requests being processed per second. It provides a comparison against the computed average for the specified time interval.</p>
Where to go next	Drill down on: <ul style="list-style-type: none"> Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Table 76. Top AD Metrics view - Roles

Description	When Roles is selected, this view displays additional data about the roles being performed by this DC.
Data displayed	<p>FSMO. A green check icon indicates whether this DC 'owns' the following operations master roles:</p> <ul style="list-style-type: none"> • Schema Master • Domain Naming Master • Infrastructure Master • RID Master • PDC Emulator <p>DNS.</p> <ul style="list-style-type: none"> • SRV Record for DC Registered. When this check box is selected it indicates that the SRV Record for the selected DC is registered. • DNS Server. When this check box is selected it indicates that this DC is a DNS Server. If the DC is a DNS server, this view also displays the rate at which queries are received and responses are sent. <p>Global Catalog.</p> <ul style="list-style-type: none"> • Global Catalog. When this check box is selected it indicates that this DC is hosting a Global Catalog. • Global Catalog Search Response. This value displays the rate at which it takes to perform a Global Catalog search.
Where to go next	Drill down on:
	Total Queries Received. (DNS Servers only) Displays a metrics popup that describes the counter and a graph that charts the number of queries received over the specified time interval.
	Total Responses Sent. (DNS Servers only) Displays a metrics popup that describes the counter and a graph that charts the number of responses sent over the specified time interval.
	Global Catalog Search Response. Displays a metrics popup that describes the counter and a graph that charts data over the specified time interval.

Top 3 Consumers view

This view is part of the Forest Environment Summary, Domain Environment Summary and Site Environment Summary, when an individual forest, domain or site is selected in the Object Tree view (Quick View) on the Active Directory Environment dashboard.

Table 77. Top 3 Consumers view

Description	The sortable lists in this view display the top three DCs in the selected forest, domain or site that are consuming the most computer resources.
Data displayed	<p>Top 3 CPU Consumers. Lists the top three DCs that are consuming the most CPU processor time. This table includes the name of the DCs and the CPU resources being consumed by each DC.</p> <p>Top 3 Memory Consumers. Lists the top three DCs that are consuming the most memory. This table includes the name of the DCs and the amount of memory being consumed by each DC.</p> <p>Top 3 Network Consumers. Lists the top three DCs that are consuming the most network bandwidth. This table includes the name of the DCs and the rate at which network resources are being consumed by each DC.</p>

Table 77. Top 3 Consumers view

Top 3 Storage Consumers. Lists the top three DCs that are consuming the most storage space. This table includes the name of the DCs and the rate at which storage resources are being consumed by each DC.

Where to go next	N/A
-------------------------	-----

Top 3 CPU Consumers view

This view is part of a Forest Explorer Summary, Domain Explorer Summary or Site Explorer Summary, which is displayed when an individual forest, domain or site is selected in the Active Directory Enterprise view on the Active Directory Explorer dashboard. This view is also displayed on the Summary views for the Forests, Domains, and Sites object containers.

Table 78. Top 3 CPU Consumers view

Description	The graph charts the CPU utilization for the top three DCs in the selected forest, domain or site. The list at the bottom of this view displays the top three DCs that are consuming the most CPU processor time during the specified time interval.
--------------------	--

Where to go next	N/A
-------------------------	-----

Top 3 DS Directory Reads/sec view

This view is part of a Forest Explorer Summary, Domain Explorer Summary or Site Explorer Summary, which is displayed when an individual forest, domain or site is selected in the Active Directory Enterprise view on the Active Directory Explorer dashboard.

Table 79. Top 3 DS Directory Reads/sec view

Description	The graph charts the number of directory reads per second for the top three DCs in the selected forest, domain or site. The list at the bottom of this view displays the top three DCs that are generating the most directory reads during the specified time interval.
--------------------	---

Where to go next	N/A
-------------------------	-----

Top 3 LDAP Bind Times view

This view is part of a Forest Explorer Summary, Domain Explorer Summary or Site Explorer Summary, which is displayed when an individual forest, domain or site is selected in the Active Directory Enterprise view on the Active Directory Explorer dashboard.

Table 80. Top 3 LDAP Bind Times view

Description	The graph charts how long (in milliseconds) it took to perform the last successful LDAP bind request on the top three DCs in the selected forest, domain or site. The list at the bottom of this view displays the top three DCs that took the longest to perform the last successful LDAP bind request during the specified interval.
--------------------	--

Where to go next	N/A
-------------------------	-----

Top 3 Memory Consumers view

This view is part of a Forest Explorer Summary, Domain Explorer Summary or Site Explorer Summary, which is displayed when an individual forest, domain or site is selected in the Active Directory Enterprise view on the Active Directory Explorer dashboard.

Directory Explorer dashboard. This view is also displayed on the Explorer Summary views for the Forests, Domains, and Sites object containers.

Table 81. Top 3 Memory Consumers view

Description	The graph charts the memory utilization for the top three DCs in the selected forest, domain or site. The list at the bottom of this view displays the top three DCs that are consuming the most memory during the specified time interval.
Where to go next	N/A

Top 3 Network Consumers view

This view is part of a Forest Explorer Summary, Domain Explorer Summary or Site Explorer Summary, which is displayed when an individual forest, domain or site is selected in the Active Directory Enterprise view on the Active Directory Explorer dashboard. This view is also displayed on the Explorer Summary views for the Forests, Domains, and Sites object containers.

Table 82. Top 3 Network Consumers view

Description	The graph charts the network utilization for the top three DCs in the selected forest, domain or site. The list at the bottom of this view displays the top three DCs that are consuming the most network bandwidth during the specified time interval.
Where to go next	N/A

Top 3 Replication Queue Length view

This view is part of a Forest Explorer Summary, Domain Explorer Summary or Site Explorer Summary, which is displayed when an individual forest, domain or site is selected in the Active Directory Enterprise view on the Active Directory Explorer dashboard.

Table 83. Top 3 Replication Queue Length view

Description	The graph charts the replication queue lengths for the top three DCs in the selected forest, domain or site. The list at the bottom of this view displays the top three DCs that have the longest replication queue lengths during the specified time interval.
Where to go next	N/A

Top 3 Storage Consumers view

This view is part of a Forest Explorer Summary, Domain Explorer Summary or Site Explorer Summary, which is displayed when an individual forest, domain or site is selected in the Active Directory Enterprise view on the Active Directory Explorer dashboard. This view is also displayed on the Explorer Summary views for the Forests, Domains, and Sites object containers.

Table 84. Top 3 Storage Consumers view

Description	The graph charts the storage utilization for the top three DCs in the selected forest, domain or site. The list at the bottom of this view displays the top three DCs that are consuming the most storage space during the specified time interval.
Where to go next	N/A

Trusts view

This embedded view is part of the Forest Environment Summary and Domain Environment Summary when an individual forest or domain is selected in the Object Tree view (Quick View) on the Active Directory Environment dashboard.

Table 85. Trusts view

Description	This view contains a list of inbound and outbound trusts established for the selected forest or domain.
Data displayed	Inbound. Displays the name of the forests/domains that trust the current forest or domain. Outbound. Displays the name of the forests/domains that the current forest or domain trusts. Type. For both Inbound and Outbound trusts, this column displays the state of each trust relationship: <ul style="list-style-type: none">• Tree Root - the trust relationship is between two tree root domains in the forest.• Parent - the trust relationship is from a parent domain to a child domain.• Child - the trust relationship is from a child domain to a parent domain.• External - the trust relationship is with a pre-Windows 2000 (NT) domain.• Non-Windows Kerberos Realm - the trust relationship is with a Kerberos realm, which is a standard security and authentication protocol.• DCE Realm - the trust relationship is with a DCE realm.• Shortcut - the trust relationship is between two domains in the same forest that are not directly related. Transitive. For both Inbound and Outbound trusts, this columns indicates whether the trust is a transitive trust. Transitive trusts can only exist between domains within the same domain tree or forest.
Where to go next	N/A

USN Records view

To display this view, enable the **USN Records Group** in the FRS section of the Metrics Management dashboard. When this collection group is enabled, this view is added to the FRS navigation tab for the selected DC in the Active Directory Explorer dashboard.

NOTE: Either a DFS-R or an FRS tab will be displayed on the Active Directory Explorer dashboard, depending on the file replication service set up for the SYSVOL on the selected DC.

Table 86. USN Records view

Description	This view displays metrics related to Update Sequence Number (USN) records on the selected DC which are gathered when the USN Records collection group is enabled.
Data displayed	USN Records. This graph charts the following metrics over the specified time interval: <ul style="list-style-type: none">• USN Reads. Shows the number of times FRS has initiated a read on the NTFRS change log.• USN Records Examined. Shows the number of times the NTFRS change log records have been examined by FRS.• USN Records Rejected. Shows the number of times the NTFS change log records have been skipped by FRS.

Table 86. USN Records view

Where to go next	Drill down on:
	<ul style="list-style-type: none">Clicking a graph in this view displays a metrics popup that describes the counters, provides more detailed data points, and lists current alarms for the selected metric.

Foglight for Active Directory rules

Foglight for Active Directory includes a number of predefined rules to monitor all critical components of Active Directory® on a continuous basis to ensure that the directory is functioning properly. The rules included in this cartridge alert you to key conditions that may affect the health of Active Directory. Foglight allows you to modify these predefined rules or create your own rules to ensure you are monitoring statistics and alerting on conditions specific to your Active Directory environment.

Foglight for Active Directory provides an additional dashboard that can be used to manage the cartridge's rules. That is, Foglight for Active Directory rules can be managed using one of the following dashboards:

- Rules dashboard (**Dashboards > Administration > Rules > All**)
- Active Directory Rule Management dashboard (**Dashboards > Active Directory > Rule Management**)

i **NOTE:** All original rules in each cartridge are reset when the cartridge is upgraded; therefore if you applied custom conditions to any original rules these modifications will be lost. It is recommended that when modifying rules you make a copy of the original, disable the original and enable the copy with the new condition. Use the copy rule icon to the far right of a rule on the Manage Rules dashboard to copy a rule.

This section describes the Active Directory Rule Management dashboard and explains the tasks that can be performed from this dashboard:

- [Rules dashboard](#)
- [Active Directory Rule Management dashboard](#)
- [Managing Foglight for Active Directory rules](#)
- [Rules reference](#)

Rules dashboard

The Rules dashboard lists all rules that exist in your environment and allows you to drill down to rule definitions. From this dashboard you can copy, edit, and remove Foglight rules.

i **NOTE:** Predefined rules may be modified during regular software updates. To avoid losing changes to these rules, we recommend copying a rule and making edits to the copy. Enable the copy and disable the original rule. You may want to identify your custom rules with a unique prefix to make them easy to find.

To review and edit rules:

- 1 In the navigation panel, under **Homes**, click **Administration**.
- 2 In the **Administration** dashboard, click **Rules > All**.
The Rules dashboard opens.
- 3 From the Cartridge list, select *Active-Directory*.
The dashboard refreshes to display only the Foglight for Active Directory rules.
- 4 From here, you can perform the following tasks:
 - Review a short description of the rule.

- Review and edit threshold values.

TIP: For rules that reference registry variables for threshold values, modify the threshold in the registry variable, rather than modifying the rule. For help finding and editing registry variables, search for “Registry Variable” in the online help.

- Copy rules.
- Edit rule conditions.
- Associate actions with rules.
- Create user-defined rules.

For help with these tasks, open the online help from the Rules dashboard.

Active Directory Rule Management dashboard

The Active Directory Rule Management dashboard contains a sortable list of all the conditional severity rules used by Foglight for Active Directory. From this dashboard you can quickly see which conditional rules are enabled/disabled, the states (fatal, critical or warning) with active conditions, predefined alarm threshold values, rules with current alarms, and a brief description of each rule.

NOTE: The Rule Management dashboard does not display simple rules that do not have user-definable conditions defining when to raise an alarm. To edit the simple rules, use the Manage Rules dashboard.

Figure 41. Active Directory Rule Management dashboard

Enabled	Rule	Fatal	Critical	Warning	Alarms	Description
<input type="checkbox"/>	Host CPU Privileged Time	75	75	75		Checks if the percentage of processor privileged time is above the thresh
<input type="checkbox"/>	Host Physical Disk sec Avg Write	1000	1000	1000		Checks if the physical disk average write time (in ms) is above the thresh
<input type="checkbox"/>	Host Network Outbound Errors	60	80	20		Checks if the number of outbound packet errors is above the threshold v
<input type="checkbox"/>	Host Logical Disk sec Avg Read	1000	1000	1000		Checks if the logical disk average read time (in ms) is above the thresho
<input type="checkbox"/>	Host CPU User Time	99	75	75		Checks if the percentage of processor user time is above the threshold v
<input type="checkbox"/>	Host CPU Utilization	95	90	75		Checks if the percentage of processor utilization is above the threshold v
<input type="checkbox"/>	DRA Inbound Full Sync Objects Remaining	2000	1000	300		DRA Inbound Full Sync Objects Remaining rule.
<input type="checkbox"/>	DRA Pending Replication Synchronizations	8	4	2		DRA Pending Replication Synchronizations rule.
<input type="checkbox"/>	Host DOT NET Framework Memory	10	10	10		Checks if the percentage of time in garbage collection (GC) is above the t
<input type="checkbox"/>	Host Logical Disk sec Avg Write	1000	1000	1000		Checks if the logical disk average write time (in ms) is above the thresho
<input type="checkbox"/>	LDAP Bind Time	400	200	80		LDAP Bind Time rule.
<input type="checkbox"/>	DRA Inbound Objects Applied Per/sec	200	100	40		DRA Inbound Objects Applied Per/sec rule.
<input type="checkbox"/>	Host Physical Disk sec Avg Read	1000	1000	1000		Checks if the physical disk average read time (in ms) is above the thresho
<input type="checkbox"/>	ESE Database Cache Size	25	25	25		ESE Database Cache Size rule.
<input type="checkbox"/>	Host Memory Percent Committed	25	25	25		Checks if the percentage of memory committed bytes is above the thresh
<input type="checkbox"/>	Host Memory Paging	25	25	25		Checks if the sum of the page in rate and the page out rate is above the
<input type="checkbox"/>	Host Network Available Bandwidth	25	25	25		Checks if the available network bandwidth is less than the threshold valu
<input type="checkbox"/>	ESE Table Open Cache Hits Per/sec	25	25	25		ESE Table Open Cache Hits Per/sec rule.
<input type="checkbox"/>	ESE Database Page Faults Per/sec	25	25	25		ESE Database Page Faults Per/sec rule.
<input type="checkbox"/>	ESE Database Cache Percent Hit	25	25	25		ESE Database Cache Percent Hit rule.
<input type="checkbox"/>	Host Processor Queue Length	25	25	25		Checks if the processor queue length is above the threshold value.
<input type="checkbox"/>	Host Memory Available	25	25	25		Checks if the memory usage is above the threshold value.
<input type="checkbox"/>	Host Storage Capacity	25	25	25		Checks if at the present growth rate the logical drive will be full within the
<input type="checkbox"/>	ESE Log Record Stalls Per/sec	25	25	25		ESE Log Record Stalls Per/sec rule.
<input type="checkbox"/>	Host Memory Pool Non Paged bytes	25	25	25		Checks if the memory pool non-paged bytes is abnormally high based on
<input type="checkbox"/>	ESE Log Writes Per/sec	25	25	25		ESE Log Writes Per/sec rule.

The Active Directory Rule Management dashboard displays the following information about Foglight for Active Directory rules.

Table 87. Active Directory Rule Management dashboard information

















Column	Description
	Use the selection check box column to select one or more rules in the list. Once selected, you can enable or disable the selected rules using the buttons at the top of the table. To select or clear all of the rules in the list, click on the check box in the heading row.
Enabled	Displays one of the following icons indicating whether the rule is enabled or disabled:  - Enabled  - Disabled Clicking the icon in this column will either disable or enable the selected rule.
Rule	Displays the name of the rule. Selecting the rule name launches the rule editor where you can view or edit the selected rule.
	Fatal Condition: <ul style="list-style-type: none"> The set rule icon  indicates that a fatal condition is not yet defined for this rule. Selecting this icon displays a dialog allowing you to specify a value for the rule or launches the rule editor allowing you to define a fatal condition for this rule. The icon  indicates multiple registry values. Clicking this icon displays a dialog that allows you to view the fatal condition threshold for these variables. The edit icon  indicates that you can define a fatal condition for this rule. Clicking this icon launches the rule editor allowing you to define a fatal condition for this rule.
	Critical Condition: <ul style="list-style-type: none"> The set rule icon  indicates that a critical condition is not yet defined for this rule. Selecting this icon displays a dialog allowing you to specify a value for the rule or launches the rule editor allowing you to define a critical condition for this rule. The icon  indicates multiple registry values. Clicking this icon displays a dialog that allows you to view the fatal condition threshold for these variables. The edit icon  indicates that you can define a fatal condition for this rule. Clicking this icon launches the rule editor allowing you to define a fatal condition for this rule.
	Warning Condition: <ul style="list-style-type: none"> The set rule icon  indicates that a warning condition is not yet defined for this rule. Selecting this icon displays a dialog allowing you to specify a value for the rule or launches the rule editor allowing you to define a warning condition for this rule. The icon  indicates multiple registry values. Clicking this icon displays a dialog that allows you to view the fatal condition threshold for these variables. The edit icon  indicates that you can define a fatal condition for this rule. Clicking this icon launches the rule editor allowing you to define a fatal condition for this rule.

Table 87. Active Directory Rule Management dashboard information

Column	Description
Alarms	<p>Indicates the number of outstanding alarms for each rule.</p> <p>Selecting the number in this column displays the alarms popup. From the alarm list on this popup:</p> <ul style="list-style-type: none"> Clicking the alarm message, time or severity icon for an individual alarm displays the Alarm Details dialog from which you can acknowledge or clear the alarm. Selecting the Info icon  displays the Metrics and Troubleshooting dialog. (When a service is stopped, the popup displays the state of the selected service at different times over the specified time interval.) Selecting a server allows you to view the performance metrics in the Active Directory Explorer or Quick View.
Available In	Indicates the Exchange version in which the rule is available.
Description	Provides a brief description of the rule.

Managing Foglight for Active Directory rules


In addition to viewing Foglight for Active Directory rules, you can edit alarm thresholds and enable/disable rules using the Active Directory Rule Management dashboard.

To disable a rule:

- 1 Locate the rule to be disabled and click the icon in the corresponding Enabled column.

NOTE: To disable multiple rules, select the corresponding check boxes to the left of the rules to be disabled and select the Disable Rule toolbar button.
- 2 On the confirmation dialog, select **Yes**.

To edit the condition of a rule:

- 1 Select the rule in the Rule column or its corresponding graph icon  in the Fatal, Critical or Warning columns.

NOTE: Hovering the cursor over a numeric value or graph icon will display the current condition that is defined.

NOTE: To define a condition for a rule, select the set rule icon in the corresponding Fatal, Critical or Warning columns.
- 2 On the Edit Rule view, edit the conditions, alarms, actions, schedules, behavior or rule variables as required. After making your edits, select **Save All**.


For more detailed information on editing rules, see the *Foglight Administration and Configuration Help*.

- NOTE:** In the browser interface, open the Help tab in the action panel. Navigate to Using Foglight > Administration and Configuration Help > Tuning Foglight for Optimal Performance > Using Foglight Rules to Report on Bottlenecks. Scroll to the bottom of that page to find a list of reference topics including procedures explaining how to perform a variety of tasks related to rules.

To edit the alarm threshold assigned to a rule:

- 1 Select the numeric value in the Fatal, Critical or Warning columns.
- 2 Enter the new value and select **Update**.

To activate/deactivate a condition for a rule:

- 1 Select the deactivated value or graph icon  in the corresponding Fatal, Critical or Warning columns.
 - If you selected a deactivated value, on the Threshold dialog, select the **Activate** check box and if desired modify the threshold value displayed. Select **Update**.
 - If you selected a deactivated graph icon, on the Edit Rule view, select the **Activate** check box on the Conditions, Alarms & Actions tab. If necessary, edit the conditions, alarms, actions, schedules, behavior or rule variable as required. After activating and/or modifying the condition, select **Save All**.
- 2 To deactivate a condition, select the rule, active value or chart icon in the corresponding Fatal, Critical or Warning columns.
 - If you selected a value, on the Threshold dialog, clear the **Activate** check box. Select **Update**.
 - If you selected a rule or a graph icon, on the Edit Rule view, clear the **Activate** check box on the Conditions, Alarms & Actions tab. After deactivating the condition, select **Save All**.

Rules reference

Foglight allows you to create flexible rules that can be applied to complex, interrelated data from multiple sources within your distributed system. You can associate several different actions with a rule, configure a rule so that it does not fire repeatedly, and associate a rule with schedules to define when it should and should not be evaluated.

Different types of data can be used in rules, including registry variables, raw metrics, derived metrics, and topology object properties.

There are two types of rules in Foglight: simple rules and multiple-severity rules. A simple rule has a single condition, and can be in one of three states: Fire, Undefined, or Normal. A multiple-severity rule can have up to five severity levels: Undefined, Fatal, Critical, Warning, and Normal.

Rule conditions are regularly evaluated against monitoring data (metrics and topology object properties collected from your monitored environment and transformed into a standard format). Therefore, the state of the rule can change if the data changes. For example, if a set of monitoring data matches a simple rule's condition, the rule enters the Fire state. If the next set does not match the condition, the rule exits the Fire state and enters the Normal state.

A rule condition is a type of expression that can be true or false. When it evaluates to true, the rule is said to fire, causing any actions that are associated with the rule or severity level to be performed. You can configure a rule to perform one or more actions upon entering or exiting each state. When a multiple-severity rule fires, an alarm also appears in Foglight.

Foglight for Active Directory includes several conditional severity rules. In addition, this cartridge may use some of the Host Monitoring rules.

i | **NOTE:** The host monitoring rules are only used if the Host Collector setting is set to AD on the agent's properties page. If the host metrics are being collected by Foglight for VMWare, Foglight for Hyper-V, or Foglight for Infrastructure, the host monitoring rules defined for that cartridge will be used instead.

For more information, see the *Foglight Administration and Configuration Guide* or online help.

Running diagnostic tests

The Foglight for Active Directory provides diagnostics tests to help you detect and analyze Active Directory® problems. Using the Diagnostic Tests dashboard, which is available in Foglight for Active Directory, you can view a list of diagnostic tests that are available as well as run a test immediately or define a schedule for when a test is to be run.

- ! **IMPORTANT:** Running diagnostic tests may impact performance. The impact on performance depends on your environment (network bandwidth, speed, etc.), the number of servers being tested, and the number of tests being run. Therefore, it is recommended to run individual tests against specific servers to analyze a particular problem.

This section describes the components of the Diagnostic Tests dashboard and explains the tasks that can be performed from this dashboard. It also provides a description of the diagnostic tests that are available in Foglight for Active Directory to detect and analyze your Active Directory environment.

- [Diagnostic Tests dashboard](#)
- [Diagnostic Tests reference](#)

Diagnostic Tests dashboard

The Diagnostic Tests dashboard allows you to run diagnostic tests against one or more servers in your Active Directory® environment.

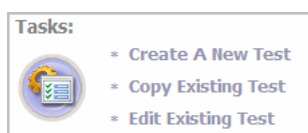
It consists of the following components:

- [Tasks list](#)
- [About Diagnostic Test Types pane](#)
- [Diagnostic Tests list](#)

Tasks list

The Tasks list in the upper left-hand corner of the dashboard contains a list of tasks that can be performed from this dashboard.

Figure 42. Task list



Clicking a task in this list launches a wizard or displays a dialog allowing you to further define the task to be performed:

- **Create a New Test** - select this task to specify the test parameters to be used to run a test. Selecting this task launches the Create New Diagnostic Test wizard which steps you through the process.

- **Copy Existing Test** - select this task to use an existing test as a basis for creating a new test. Selecting this task displays the Copy Diagnostic Test dialog allowing you to select an existing test to be copied. Once you select a test to be copied, the Create New Diagnostic Test wizard is launched allowing you to modify the test parameters as required.
- **Edit Existing Test** - select this task to modify the test parameters of an existing test. Selecting this task displays the Edit Diagnostic Test dialog allowing you to select an existing test to be modified. After selecting the test to be edited, the Edit Diagnostic Test wizard is launched allowing you to modify the test as required.

Create New Diagnostic Test

The Create New Diagnostic Test wizard allows you to select the type of test to be run and to specify the test input and the servers the test is to be run against. It also allows you to specify when the test is to be run.

To create a new test:

- 1 Select the **Create a New Test** task in the task list at the top of the dashboard to launch the Create New Diagnostic Test wizard.
- 2 On the Create New Test page, enter the following information:
 - Diagnostic Test Name - enter a descriptive name for the test to be run
 - Test Type - select the type of test to be run
 - Test Input - enter the test input as required
- 3 On the Test Targets page, select the **Select Targets** button. On the Select Targets dialog, select one or more servers and select **OK**.

i | **NOTE:** You can also select all the servers in a domain or a site, by using the View by options at the top of the dialog and selecting either a domain or site from the displayed list.
- 4 On the Test Execution Schedule page, select one of the following options to define how often the test is to be run:
 - **Run Once** - select to run the test one time when the **Finish** button is selected.
 - **Run Periodically** - select to run the test multiple times during a day. Enter how often the test is to be run (every nn minutes). To specify a start and end time, select the **Use execution window** check box and use the calendar controls to specify the start and end time.
 - **Run Once Each Day** - select to run the test every day at the specified time. Use the calendar control to specify the time.

i | **NOTE:** A test should not be re-run within 10 minutes. If you select to re-run the test within this 10 minute interval, the Test Run Frequency Warning message appears.
- 5 Select **Finish** to initiate the test run and close the wizard.

The new test appears in the Diagnostic Tests list on the Diagnostic Tests dashboard. To view the test's results, select the selection icon to the left of the test in this list.

For more information about the controls and information requested on the wizard, see [Create New Diagnostic Test Wizard](#)

Copy Existing Diagnostic Test

To copy an existing test:

- 1 Select the **Copy Existing Test** task in the task list.
- 2 On the Copy Diagnostic Test dialog, select the test to be copied and select the **Copy** button.
- 3 On the Create New Diagnostic Tests dialog, modify the following information as appropriate:

- On the first page, enter a new name for the test, select the type of test to be run and enter any test inputs.
 - On the second page, select the **Select Servers** button to select the servers on which the test is to be run.
 - On the last page, select when the test is to be run.
- 4 Select **Finish** to save your selections and close the wizard.
 - 5 The new test appears in the Diagnostic Tests list on the Diagnostic Tests dashboard.

Edit Existing Diagnostic Test

To edit an existing test:

- 1 Select the **Edit Existing Test** task in the task list.
- 2 Select the test to be modified from the Edit Diagnostic Test dialog and select **Edit** to launch the Edit Diagnostic Test wizard.
 - i** | **NOTE:** You can also select a test from the Diagnostic Test list and click the Edit toolbar button at the top of the test list to launch the Edit Diagnostic Test wizard.
- 3 Modify the settings as appropriate:
 - On the first page of the wizard, you can modify the test input parameters.
 - On the second page of the wizard, you can select a different set of servers.
 - On the last page of the wizard, you can select a different run schedule.
- 4 When complete, select the **Finish** button to save your selections and close the wizard.

Create New Diagnostic Test Wizard

This wizard is launched when you select the **Create a New Test** or **Copy Existing Test** task in the tasks list on the Diagnostic Tests dashboard.

The Create New Diagnostic Test wizard includes several pages and requires the following information:

- Create New Test: From this page, provide a name for the new test, select the test type and enter the test input.
 - Diagnostic Test Name: Enter a descriptive name for the diagnostic test.
 - Test Type: Select the type of test to be run.
 - Test Input: Depending on the type of test selected, this pane displays the test input that must be entered.
 - i** | **NOTE:** See the description of each individual diagnostic ([Diagnostic Tests reference](#)) for the test input required for each diagnostic.
- Test Targets: From this page, select the target servers on which the test is to be run.
 - i** | **NOTE:** For each test, the credentials for the domain controllers selected on this page are used to query all of the servers selected in the diagnostic. For diagnostics that query additional servers (i.e., replication partners, the PDC Emulator or Schema Master), all the servers must be within the same forest and the account used must have access to all the selected servers.
 - NOTE:** For the File Replication and Track Replication diagnostics, select only one target server.
 - Select Targets: Selecting this button displays the Select Targets dialog which lists the servers which are being monitored by an Active Directory® agent.
 - i** | **NOTE:** This list will not include servers that host an Active Directory agent which has not yet reported any data. It will also list servers that may not be currently running, but have previously collected data.

Use the **View by** option at the top of the dialog to display the available servers. Depending on this setting, you can select one or more servers, all servers in a domain or all servers in a site.

- View by Servers - allows you to select one or more individual servers or all servers.
- View by Sites - allows you to select one or more individual servers or a site to include all servers in that site
- View by Domains - allows you to select one or more individual servers or a domain to include all servers in that domain.

After selecting the target servers to be tested, use the **OK** button to close the dialog and return to the wizard.

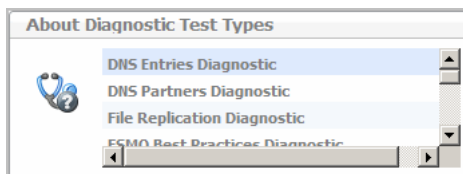
Once a target is selected, the following information is displayed:

- Type - indicates whether a server, domain or site was selected on the Select Targets dialog.
 - Name - displays the name of the selected server(s), domain(s), or site(s).
- Test Execution Schedule: From this page, specify how often the test is to be run.
 - Run Once: Select to run the test one time when the **Finish** button is clicked.
 - Run Periodically: Select to run the test multiple times during the day. Enter the following information to specify when the test is to be run during the day:
 - **Run every nn minutes** - enter the number of minutes
 - **Use execution window** - select this check box and use the calendar controls to specify the start and end time.
 - Run Once Each Day: Select to run the test once each day and use the calendar control to select the time the test is to be run.

About Diagnostic Test Types pane

The About Diagnostic Test Types pane in the upper right corner of the dashboard displays a list of test types available.

Figure 43. About Diagnostic Test Types



Selecting a test type from this list displays a pop-up which provides a brief description of the selected test.

Diagnostic Tests list

The remainder of this dashboard consists of the Diagnostic Tests list. As tests are created using the **Create A New Test** task, the test parameters as specified in the wizard will be displayed for each new test created. From this list, you can select the **Run Now** icon to run the test or select a test to view the test results.

Figure 44. Diagnostic Tests list

Diagnostic Tests - Select "Run Now" icon to run selected test and then select test to see result.

Test	Run Now	Last Run Time	Schedule	Test Type
DNS Entries - Fri		7/11/11 2:28 PM	Run Periodically	DNS Entries Diagnostic
FSMO BP		7/11/11 2:11 PM	Run Periodically	FSMO Best Practices Diagnostic
Parent Time Sync		7/11/11 12:44 PM	Run Once Each Day	Time Parent Sync Diagnostic
Time Differential		7/11/11 1:45 PM	Run Once Each Day	Time Differential Diagnostic

Parent Time Sync - Select "View Results" icon to view details for each item.

Test Runs	View Results	Status	Message
Parent Time Sync			
<div>FITZGERALD</div> <div>7/11/11 12:44 PM</div>		Success	
<div>EVEREST</div> <div>7/11/11 12:44 PM</div>		Success	
<div>HALL</div> <div>7/11/11 12:44 PM</div>		Success	
<div>MAKALU</div> <div>7/11/11 12:44 PM</div>		Success	
AND-EVEREST			

The Diagnostic Tests list contains the following information for each test that has been scheduled to run.

Table 88. Diagnostic Tests list information

Column	Description
	Select the selection icon for a test to display an additional panel at the bottom of the page to display the results of the selected test. See Test results for a description of the additional details displayed. Selecting a test also enables the Edit and Delete toolbar buttons allowing you to remove the test from the list or edit the test to be run.
Test	Displays the name of test as entered on the first page of the wizard.
Run Now	Click the icon in this column to initiate a test run. NOTE: A test should not be re-run within 10 minutes. If you select to re-run the test within this 10 minute interval, the Test Run Frequency Warning message appears. NOTE: If agent data collection is turned off for the selected target server, the test will fail. If you start the data collection for the server and run the test within the 10 minute interval, the Test Run Frequency Warning message appears. Use the Override button to run the test now that the agent data collection is turned on.
Last Run Time	Indicates the date and time when the test was last run.
Schedule	Displays the test execution schedule as specified in the wizard.
Test Type	Displays the type of test.


Test results

The following details are displayed at the bottom of the Diagnostic Tests dashboard when a test is selected in the Diagnostic Tests list.

Table 89. Test results

Column	Description
Test Name	The name of the selected test is displayed across the top of this pane.
Test Runs	Displays the servers tested and the dates and times when the test was run. Select the expansion button to the left of a test to display a list of the test runs that have been performed against each server.

Table 89. Test results

Column	Description
View Results	Click the  icon in this column to view the detailed test results. <ul style="list-style-type: none"> • Test - clicking the icon for a test displays results for the entire test, including all servers and all test runs. • Server - clicking the icon for a server displays results for all runs for the selected server. • Test Run - clicking the icon for a test run displays results for the selected test run on that server.
Status	Display the overall status of each test run. The following icons are used to illustrate each status: <ul style="list-style-type: none"> • Success (Green) - indicates the test completed successfully • Failed (Red) - indicates that the test failed to complete
Message	Displays progress messages generated during a test run.

Diagnostic Tests reference

This section provides a description of the diagnostic tests available in Foglight for Active Directory:

- [DNS Entries diagnostic](#)
- [DNS Partners diagnostic](#)
- [File Replication diagnostic](#)
- [FSMO Best Practices diagnostic](#)
- [GPO Sync diagnostic](#)
- [Hotfix and Service Pack diagnostic](#)
- [Replication Failure diagnostic](#)
- [Replication Link diagnostic](#)
- [Schema Consistency diagnostic](#)
- [Service Status diagnostic](#)
- [Site Configuration diagnostic](#)
- [Time Differential diagnostic](#)
- [Time Parent Sync diagnostic](#)
- [Track Replication diagnostic](#)

DNS Entries diagnostic

Verifies that the DNS entries registered by a specific domain controller can be found on the DNS servers. It finds and parses the following file for pertinent DNS information (which should work for non-MS DNS references):

C:\Windows\System32\config\netlogon.dns. This functionality is mostly redundant with the reported 'isSrvRegistered' value for each given domain controller.

If this test fails, you should:

- Ensure that the selected server is operational.

- Ensure that you have access to the admin\$ share on the selected server. This test requires access to the netlogon.dns file stored in admin\$\System32\config.
- Verify that you can make DNS requests from your computer. This test contacts the default DNS server for the local computer.

DNS Partners diagnostic

Verifies that the DC can find the DNS records of each of its inbound replication partners on the DNS server that it is using. To accomplish this, the test works in unison with LDAP and NSLOOKUP utilities.

If this test fails, you should:

- Ensure that the DC and its partners are operational.
- Ensure LDAP connectivity is available against the target DC (access via ntdsConnection object).
- Verify (either using nslookup or the Microsoft® DNS snap-in) that the entries are actually registered.

File Replication diagnostic

Allows you to check the presence of any file on other domain controllers. This test verifies that the files stored on all shares are physically the same files. It verifies the file size in bytes, file date, and file name between the source server and all other selected servers.

To run this test, select the replication partners and enter the name of the file or folder you want confirmed. The test continues through all DCs, recording errors as it processes differences that are found.

i | NOTE: Select only one target server when running this test.

Table 90. File Replication diagnostic

Test Input	Description
Select Replication Partners	Select this button to select the servers where tests should compare the most recent update with that of the target server. Selecting this button displays the Select Target dialog which provides a list of replication partners to choose from. NOTE: The credentials for the domain controller selected on the Test Targets page will be used to query the replication partner servers selected here. Therefore, the user account used by the selected target server must also have access to these replication partners. NOTE: Be sure to select servers (both the target servers and replication partners) that are within the same forest. Selecting servers that reside in different forests will result in communication errors.
File Name	Enter the name of the file or folder you want to compare. Enter in the following format: c:/Windows/System32/drivers/etc/hosts
Compare File Size	This check box is selected by default indicating that the diagnostic test is to compare the file size. Clear this check box if you do not wish to compare the file size.
Compare File Date	This check box is selected by default indicating that the diagnostic is to compare the file date. Clear this check box if you do not wish to compare the file date.

If this test fails, you should:

- Ensure that you have access to the admin\$ share on the selected server.

FSMO Best Practices diagnostic

Tests to determine whether the target domain controllers are following FSMO best practice guidelines.

To run this test, select the best practices to be verified. All best practices are selected by default.

Table 91. FSMO Best Practices diagnostic

Test Input	Description
Verify that the PDC Emulator and RID Master roles are on the same domain controller	When selected, the test check if both of these roles are located on the same domain controller.
Verify that the Schema Master and the Domain Naming Master roles are on the same domain controller	When selected, the test checks if the Schema Master is also holding the Domain Naming Master role.
Verify that the Infrastructure Master is not a Global Catalog	When selected, the test checks if any domain controllers that hold the Infrastructure Master also hosts a copy of the Global Catalog.

GPO Sync diagnostic

Compares the file and directory version of each group policy from the selected DCs to the version found on the PDC Emulator. This test shows if the following GPO properties are inconsistent across any of the selected DCs in the forest:

- Sysvol user version
- Sysvol machine version
- Directory Services user version
- Directory Services machine version

i **NOTE:** The credentials for the domain controller(s) selected on the Test Targets page will be used to query the PDC Emulator. Therefore, the user account used by the selected target server(s) must also have access to the PDC Emulator.
If the PDC Emulator is in the list of target domain controllers, it will be skipped as the PDC Emulator is the source to which group policies are compared.

If this test fails, you should:

- DCs that failed the test may not have received replication updates from their partners. Try forcing replication between the affected DC and its partner.
- Check for replication failures on the affected DC.
- Ensure that you have administrative access to the registry on the DC. The Sysvol location is stored in the remote registry.
- Ensure that you have access to the file system on the DC. The file portion of the GPOs is read from the Sysvol container on the remote DC.

Hotfix and Service Pack diagnostic

Uses the remote registry service to enumerate all installed hot fixes and service packs on a domain controller. This is then compared to what the user selected to determine if any service packs or hot fixes are missing. If any service packs or hot fixes are missing, the test will return as a failure and provide a list of the missing entries.

When you run this test, enter a service pack number and a Microsoft® Knowledgebase Article Number.

Table 92. Hotfix and Service Pack diagnostic

Test Input	Description
Service Packs	Using the appropriate box, enter the service pack number to be verified. <ul style="list-style-type: none">• Windows® 2003• Windows 2008• Windows 2008 R2
Hot Fixes	Enter the hotfix(es) to be verified. When entering multiple hot fixes, enter as a comma separated string (e.g., KB981391, KB218436)

If this test fails, you should:

- Verify that you have administrative access to the registry on the remote DC.
- Verify that you have access to the WMIC command utility on the remote DC.
- Install the missing hotfix or service pack on the selected DC and re-run the test.

Replication Failure diagnostic

Checks all replication links for any errors that occurred in the last replication attempt.

If this test fails, you should:

- Check to ensure the DC is running and is connected to the network.
- Check if you can connect to the DC through Microsoft® native tools (ADSIEdit, Sites and Services, etc.). If you cannot connect using these tools, verify that you have administrative access to bind to that computer.

Replication Link diagnostic

Ensures connectivity across all selected replication links.

i | **NOTE:** If you run this test on a computer that is offline, you may receive an error:

If this test fails, you should:

- Check to see if the replication partner is operational.
- Check if the replication partner can be contacted by the target computer.
- Run the Find Replication Failures test to see if there have been replication problems in the past.
- Run the Check W32Time Differential test to see if there is a time synchronization problem causing the failure.
- Check that the appropriate directory records exist across the test set ('ntdsConnection' LDAP object), for incoming and outgoing replication partners.

Schema Consistency diagnostic

Checks all target domain controllers against the Schema Master to ensure schema consistency.

- i** | **NOTE:** The credentials for the domain controller(s) selected on the Test Targets page will be used to query the server hosting the Schema Master. Therefore, the user account used by the selected target server(s) must also have access to the server hosting the Schema Master.

Service Status diagnostic

Determines the state of Windows® services.

When you run this test, select the services that are to be checked to ensure they are running on all selected domain controllers.

Table 93. Service Status diagnostic

Test Input	Description
Select Services	Select this button to select the services to be checked. Selecting this button displays the Select Services dialog which displays a list of all existing services on the query server.

If this test fails, you should:

- Try connecting to the Service Control Manager through Microsoft® native tools (services.msc). If you cannot connect, verify that you have administrative access to the selected DC.
- Physically restart the affected services on the DC.

Site Configuration diagnostic

Checks the following site settings:

- **Intersite Topology Generation is disabled** - checks all selected sites to determine if Intersite Topology Generation is disabled.
- **Intrasite Topology Generation is disabled** - checks all selected sites to determine if Intrasite Topology Generation is disabled.
- **Exchange Server to Global Catalog ratio has been exceeded** - enumerates all Exchange Servers and Global Catalogs in the target site and produces an Exchange Server to Global Catalog ratio. This ratio is then compared to the user-defined ratio. If the actual ratio is greater than the predefined ratio the test will return as a failure.

If this test fails, you should:

- Place at least one domain controller in every site, and make at least one domain controller in each site a global catalog. Otherwise, it is recommended that universal group membership caching be enabled.
- Verify that the Exchange server to Global Catalog ratio does not exceed 4:1 in the given site.
- Verify that inter- and intra-site topology management are not disabled. When these generators are disabled, configuration must be performed manually, which can result in common mistakes.

Time Differential diagnostic

Compares the time of the selected domain controllers to the PDC Emulator and then compares this to the specified threshold. If the threshold is exceeded, the test will return as a failure. This test shows you child DCs whose time is not synchronized with their parent time server within a user-defined margin.

- NOTE:** The credentials for the domain controller(s) selected on the Test Targets page will be used to query the PDC Emulator. Therefore, the user account used by the selected target server(s) must also have access to the PDC Emulator.

To run this test enter a time differential that represents an acceptable threshold.

Table 94. Time Differential diagnostic

Test Input	Description
Acceptable Time Difference (seconds)	Enter the time differential (in seconds) that represents an acceptable threshold for you environment. By default, the acceptable time difference is 2 seconds.

If this test fails, you should:

- Ensure that the server is operational.
- Check to make sure your time differential threshold is set to the correct setting (default is 2 seconds).
- Check the properties of the server to see which computer is its time sync partner. If necessary, change the Time Sync parameters of the server to point to a different server.

Time Parent Sync diagnostic

Ensures that the selected domain controllers are using the PDC Emulator from their domain as their time source. The root PDC Emulator cannot be tested against external time sources. This test shows you any DC that is not synchronizing time with the Windows® default time server. The Windows default time server is the PDC Emulator in its domain. If the selected DC is the PDC Emulator for the domain, the Windows default time server is the PDC Emulator of the root domain.

- NOTE:** The credentials for the domain controller(s) selected on the Test Targets page will be used to query the PDC Emulator. Therefore, the user account used by the selected target server(s) must also have access to the PDC Emulator.

- NOTE:** If the DC is running on a guest OS (is virtual), it is possible it synchronizes with external hardware. Foglight for Active Directory will notify if VMware® services are running to aid in recognizing this possibility.

If this test fails, you should:

- Ensure that the server is operational.
- Verify that you have administrative access to the file system. The test attempts to connect to the file system on the remote server.
- Ensure that you have access to query the registry on the remote server. The test requires access to the registry to determine the server's time sync settings.
- Check to make sure you have access to query the domain object for that server. The test attempts to find the Windows 2000 default parent for a particular server by binding to objects in Active Directory® (starting with the object for the domain the server is in).
- If required, change the parameters of the server to point to the Windows 2000 default Time Sync server (for example, Resolve | Time Sync - | Set Parameters).

Track Replication diagnostic

Tracks as the selected object is replicated to all outgoing replication partners. This test determines if appropriate servers in the forest have the selected copy of an Active Directory® object. The Update Sequence Number (USN)/source computer pair for each property on the selected object is recorded from the source computer. This ensures that the tested computer has received all changes made to the object on the source computer.

i | **NOTE:** Select only one target server when running this test.

To run this test select the replication partners in the test input panel.

Table 95. Track Replication diagnostic

Test Input	Description
Select Replication Partners	<p>Select this button to select the servers where tests should compare the most recent update with that of the target server. Selecting this button displays the Select Targets dialog which provides a list of replication partners to choose from.</p> <p>NOTE: The credentials for the domain controller selected on the Test Targets page will be used to query the replication partner servers selected here. Therefore, the user account used by the selected target server must also have access to these replication partners.</p> <p>NOTE: Be sure to select servers (both the target servers and replication partners) that are within the same forest. Selecting servers that reside in different forests will result in communication errors.</p>

i | **NOTE:** When tracking an object in the domain naming context, Global Catalog servers outside the domain might fail the test. Any Global Catalog server in the forest will fail the test if it does not have the selected copy of an Active Directory object.

Managing Active Directory metrics

Active Directory® agents collect metrics by default which are then displayed throughout the Foglight for Active Directory views. In addition, Active Directory agents can be configured to collect other metrics in addition to those being collected by default.

IMPORTANT: Enabling optional metric collections may impact performance. Therefore, it is recommended to only enable the collection groups required to pinpoint a specific issue and then disable the metric collections for these collection groups once the issue is found/resolved.

Foglight for Active Directory provides a new dashboard, Active Directory Metrics Management dashboard, which allows you to view and manage the metrics that can be optionally collected by an Active Directory agent. Optional Active Directory metrics can only be enabled or disabled using this new dashboard. However, data collection schedules can be modified using any of the following dashboards.

- Agent Status dashboard (**Dashboards > Administration > Agents > Agent Status**)
- Agent Properties dashboard (**Dashboards > Administration > Agents > Agent Properties**)
- Active Directory Metrics Management Dashboard (**Dashboards > Active Directory Environment > Administration tab > Metrics Management**)

NOTE: When using the default data collection schedule (defaultSchedule), you can use the Agent Status, Agent Properties or Metrics Management dashboard to modify a data collection interval. However, when using a user-defined data collection schedule, you must use the Agent Status or Agent Properties dashboard to modify a data collection interval.

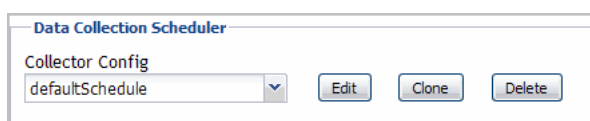
This section describes the components on the Active Directory Metrics Management dashboard. It also provides procedures for enabling and disabling metric collections and for modifying the data collection interval to be used to collect metrics:

- [Agent Status and Agent Properties dashboards](#)
- [Active Directory Metrics Management dashboard](#)
- [Managing Active Directory metrics](#)

Agent Status and Agent Properties dashboards

Similar to other cartridges, the Agent Status and Agent Properties dashboards allow you to edit an agent's properties. Use the Data Collection Scheduler setting on these dashboards to modify the data collection schedule to be used to collect performance metrics.

Figure 45. Data Collection Scheduler



Use the controls in this panel as described in the following table.

Table 96. Data Collection Scheduler controls

Control	Description
Collector Config	Specifies the data collection schedule to be used to collect performance metrics.
Edit	Select this button to edit the data collection schedule selected in the Collector Config field.
Clone	Select this button to create a copy of the data collection schedule selected in the Collector Config field. This schedule can then be used as a basis for creating a new data collection schedule.
Delete	Select this button to delete the data collection schedule selected in the Collector Config field.

Active Directory Metrics Management dashboard

The Active Directory Metrics Management dashboard lists the metrics that can be optionally collected by an Active Directory® agent. Using this dashboard, you can enable these metrics to pinpoint specific performance issues or to modify the interval to be used to collect data.

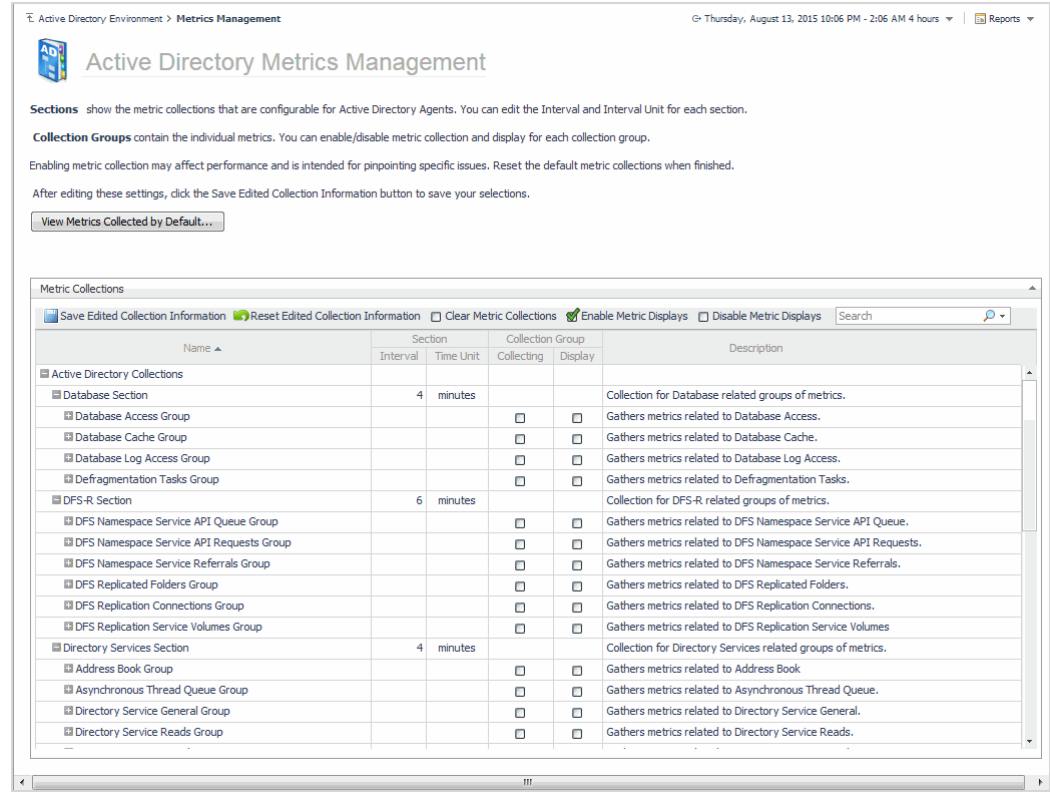
The metrics displayed on the Active Directory Metrics Management dashboard are divided into the following components:

- Sections show the metric collections that are configurable for Active Directory agents. Using the Metrics Management dashboard, you can modify the interval and time unit for each section which defines when data is to be collected.
- Collection Groups contain the individual metrics. Using the Metrics Management dashboard, you can enable or disable collection groups. Once enabled, you can also specify to display the collected metrics in a collection group on the Active Directory views.

i **NOTE:** The content of the Metrics Management dashboard is attached to the default data collection schedule (defaultSchedule) property for an agent. If a user-defined data collection schedule is being used to collect metrics, you must use the Data Collection Scheduler setting on an agent's properties page to manage the data collection schedule.

NOTE: The metrics that are collected and displayed by default are NOT displayed on the Active Directory Metrics Management dashboard, because they cannot be disabled.

Figure 46. Active Directory Metrics Management dashboard





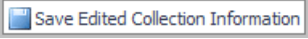




The Active Directory Metrics Management dashboard contains the following information for each collection metric.

Table 97. Active Directory Metrics Management dashboard

Column	Description
Name	<p>Lists the Active Directory Collections and when expanded, the sections, collection groups and individual metrics included in each collection group.</p> <p>To expand the Active Directory Collections to display the sections, collection groups and individual metrics, click the expansion box to the far left of the collection, section or collection group name.</p>
Section	<p>Displays the interval and time unit to be used to collect data. By default, the interval and time unit displayed are the default settings defined in the defaultSchedule.</p> <p>NOTE: Changing the interval or time unit on the Metrics Management dashboard will also change the collection interval for the corresponding collector on the Agent Properties page.</p>
Collection Group	<p>Indicates whether the metrics in the collection group are to be collected and/or displayed.</p> <ul style="list-style-type: none">Collecting - A green check mark in this column indicates that the metrics in the collection group are to be collected.Display - A green check mark in this column indicates that the metrics in the collection group are to be displayed. <p>NOTE: You can only enable the display after the collecting flag has been enabled for a collection group.</p>
Description	<p>Displays a brief description of each section, collection group, and individual metric.</p>

Use the buttons on this dashboard as described in the following table.

Table 98. Active Directory Metrics Management dashboard buttons

Button	Description
	Displays the Active Directory Default Metrics dialog which contains a list of all the metrics being collected and displayed by default.
	Rolls back unsaved changes made to any settings on the Metrics Management page to their original values.
	Saves changes made to any setting on the Metrics Management page.
	Resets the collection group settings (Collecting and Display) for the metrics in all manually enabled collection groups.
	Enables the display of the metrics in all manually enabled collection groups. NOTE: You can only enable the display after the collecting flag has been enabled for a collection group.
	Disables the display of the metrics in all manually enabled collection groups.
	Use the search control to filter the information displayed on the Metrics Management dashboard.

Managing Active Directory metrics

You can only use the Metrics Management dashboard to enable or disable the collection and/or display of optional performance metrics. However, depending on the data collection schedule being used to collect metrics, you can use the Agent Status (agent properties page), Agent Properties or Metrics Management dashboard to modify a collection interval.

- When using the default data collection schedule (defaultSchedule), you can use the Agent Status, Agent Properties or Metric Management dashboard to modify data collection intervals.
- When using a user-defined data collection schedule, you must use the Agent Status or Agent Properties dashboard to manage data collection schedules.

For details, see these topics:

- [Using the Metrics Management dashboard](#)
- [Using the Agent Status and Agent Properties dashboards](#)

Using the Metrics Management dashboard

Using the Active Directory Metrics Management dashboard, you can modify the interval and time unit for metric sections, enable/disable the collection of optional metrics in collection groups, or specify to display the collected metrics in a collection group.

To display this dashboard, select **Active Directory Environment > Administration tab > Metrics Management** from the dashboards listed in the navigation pane.

To modify the interval or time unit of a section:

i | **NOTE:** You can only modify the interval or time unit for a section, not collection groups or individual metrics.

- 1 From the Active Directory Metrics Management page, locate the section whose interval or time unit is to be modified.

- 2 To change the interval, select the value displayed in the **Interval** column. Enter the new value in the dialog and select **Update**.
- 3 To change the time unit, select the value displayed in the **Time Unit** column. Select the new time unit (days, hours or minutes) in the dialog and select **Update**.
- 4 Select the **Save Edited Collection Information** toolbar button to save your selections.

i | **NOTE:** Modifying the interval or time unit using the Metrics Management page also modifies the collection interval for the corresponding collector in the defaultSchedule (Agent Properties page).

To enable the collecting or display of optional metrics:

i | **NOTE:** You can only enable a collection group, not individual metrics within a collection group.

NOTE: Enabling metrics may affect performance. It is recommended that you only enable metrics in order to pinpoint a specific issue and to then reset the default metric collections when finished.

- 1 From the Active Directory Metrics Management page, locate the collection group to be enabled.
- 2 Click the check box in the corresponding **Collection Group | Collecting** cell.
- 3 Select the check box in the metric's collection dialog and select **Update**.

A green check mark is displayed in the **Collection Group | Collecting** column back on the Metrics Management page.

Once the collecting of a collection group is enabled, you can then enable the display of these metrics.

- 4 Click the check box in the corresponding **Collection Group | Display** column.
- 5 Select the check box in the metric's display dialog and select **Update**.

A green check mark is displayed in the **Collection Group | Display** column back on the Metrics Management page.

i | **NOTE:** If you enabled the collecting of multiple collection groups and want to enable the display of all these metrics, you can use the Enable Metric Display toolbar button instead of enabling them all individually.

- 6 Select the **Save Edited Collection Information** toolbar button to save your selections.
- 7 On the Save dialog, click **Save** to confirm that you want to save your selection.
- 8 A Save Collections dialog appears informing you that your selection(s) have been saved. Click the close button in the upper right-hand corner to close the dialog and return to the Active Directory Metrics Management dashboard.

To disable the collecting or display of optional metrics:

- 1 From the Active Directory Metrics Management page, locate the collection group to be disabled.
- 2 Click the enabled check box (contains a green check mark) in the corresponding **Collection Group** column (**Collecting** or **Display**).
- 3 Clear the check box on the dialog and select **Update**.
The green check mark is cleared from the selected column back on the Metrics Management page.
- 4 Select the **Save Edited Collection Information** toolbar button to save your selections.
- 5 On the Save dialog, click **Save** to confirm that you want disable the selected metric collection.
- 6 A Save Collections dialog appears informing you that your selection(s) have been saved. Click the close button in the upper right-hand corner to close the dialog and return to the Active Directory Metrics Management dashboard.

i | **NOTE:** To disable the collection and display of all previously enabled collection groups, use the Clear Metric Collections toolbar button.

To display the metrics being collected by default:

- 1 From the Active Directory Metrics Management page, select the **View Metrics Collected by Default** button.
- 2 The Active Directory Default Metrics dialog appears which lists the metrics that are being collected and displayed by default.

i | **NOTE:** Metrics being collected and displayed by default cannot be disabled using the Metrics Management dashboard.

- 3 To close this dialog, select the close button in the upper right-hand corner of the dialog.

Using the Agent Status and Agent Properties dashboards

On the agent's properties page, you can use the Data Collection Scheduler setting to define the data collection schedule to be used or to modify a data collection interval.

To display an agent's properties page, use one of the following methods:

- From the navigation panel, navigate to **Dashboards > Administration > Agents > Agent Status**. On the Agent Status dashboard, select an agent from the list and click **Edit Properties**. The Agent Status dashboard refreshes, showing the current properties for the selected agent instance.
- From the navigation panel, navigate to **Dashboards > Administration > Agents > Agent Properties**. On the Agent Properties dashboard, select an agent. The Properties panel is displayed, showing the current properties for the selected agent instance.

To modify the data collection interval:

- 1 Open the agent's properties page.
 - i** | **NOTE:** If accessing this page through the Agent Status dashboard, select **Modify the properties for all ExchangeAgent agents** to activate the properties on the page.
- 2 The defaultSchedule in the Data Collection Scheduler panel defines the default collection intervals being used to collect metrics. To change one or more collection intervals in the default data collection schedule, select the **defaultSchedule** and click **Edit**.

The Collector Config dialog appears, which lists all of the collectors and their current settings.

i | **NOTE:** A zero value means that the collector is turned off and is not collecting data.

- To edit a collection interval, double-click the Default Collection Interval cell of the collector to be changed, and enter a different value.
- After editing the collection interval, select **Save Changes**.
- Click the close button in the upper right corner to close the dialog.

i | **NOTE:** Advanced users can add custom collectors using the developers kit. See the Foglight online help for details.

- 3 Back on the Agent Status/Agent Properties dashboard, select **Save** to save your selections.

For more information on using these dashboards to edit an agent's properties, see the *Foglight Administration and Configuration Guide* or online help.

We are more than just a name

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

Our brand, our vision. Together.

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

Contacting Quest

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

Technical support resources

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

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

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