

Foglight™ for Citrix XenDesktop and XenApp
7.3.0

User Guide



© 2024 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 Where next meets now are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. "Apache HTTP Server", Apache, "Apache Tomcat" and "Tomcat" are trademarks of the Apache Software Foundation. Google is a registered trademark of Google Inc. Android, Chrome, Google Play, and Nexus are trademarks of Google Inc. Red Hat, JBoss, the JBoss logo, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries. CentOS is a trademark of Red Hat, Inc. in the U.S. and other countries. Fedora and the Infinity design logo are trademarks of Red Hat, Inc. Microsoft, .NET, Active Directory, Internet Explorer, Hyper-V, Office 365, SharePoint, Silverlight, SQL Server, Visual Basic, Windows, Windows Vista and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. AIX, IBM, PowerPC, PowerVM, and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Java, Oracle, Oracle Solaris, PeopleSoft, Siebel, Sun, WebLogic, and ZFS are trademarks or registered trademarks of Oracle and/or its affiliates in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries. Products bearing the SPARC trademarks are based on an architecture developed by Oracle Corporation. OpenLDAP is a registered trademark of the OpenLDAP Foundation. HP is a registered trademark that belongs to Hewlett-Packard Development Company, L.P. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries. Novell and eDirectory are registered trademarks of Novell, Inc., in the United States and other countries. VMware, ESX, ESXi, vSphere, vCenter, vMotion, and vCloud Director are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Sybase is a registered trademark of Sybase, Inc. The X Window System and UNIX are registered trademarks of The Open Group. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. "Eclipse", "Eclipse Foundation Member", "EclipseCon", "Eclipse Summit", "Built on Eclipse", "Eclipse Ready" "Eclipse Incubation", and "Eclipse Proposals" are trademarks of Eclipse Foundation, Inc. IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Apple, iPad, iPhone, Mac OS, Safari, Swift, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Ubuntu is a registered trademark of Canonical Ltd. Symantec and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. OpenSUSE, SUSE, and YAST are registered trademarks of SUSE LCC in the United States and other countries. Citrix, AppFlow, NetScaler, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. AlertSite and DéjàClick are either trademarks or registered trademarks of Boca Internet Technologies, Inc. Samsung, Galaxy S, and Galaxy Note are registered trademarks of Samsung Electronics America, Inc. and/or its related entities. MOTOROLA is a registered trademark of Motorola Trademark Holdings, LLC. The Trademark BlackBerry Bold is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Quest is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited. Ixia and the Ixia four-petal logo are registered trademarks or trademarks of Ixia. Opera, Opera Mini, and the O logo are trademarks of Opera Software ASA. Tevron, the Tevron logo, and CitraTest are registered trademarks of Tevron, LLC. PostgreSQL is a registered trademark of the PostgreSQL Global Development Group. MariaDB is a trademark or registered trademark of MariaDB Corporation Ab in the European Union and United States of America and/or other countries. Vormetric is a registered trademark of Vormetric, Inc. Intel, Itanium, Pentium, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Debian is a registered trademark of Software in the Public Interest, Inc. OpenStack is a trademark of the OpenStack Foundation. Amazon Web Services, the "Powered by Amazon Web Services" logo, and "Amazon RDS" are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries. Infobright, Infobright Community Edition and Infobright Enterprise Edition are trademarks of Infobright Inc. POLYCOM®, RealPresence® Collaboration Server, and RMX® are registered trademarks of Polycom, Inc. All other trademarks and registered trademarks are property of

their respective owners.

Legend

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

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

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

Foglight for Citrix XenDesktop and XenApp User Guide
Foglight Version - 7.3.0
Cartridge Version - 7.3.0

Contents

Getting started	6
Before you begin	6
Introducing the XenDesktop infrastructure	6
Monitoring XenDesktop components	7
Setting up data collection agents	9
Exploring administration tasks	9
Discovering XenDesktop sites	11
Creating NetScaler Agent instances	14
Exploring and managing monitoring agents	16
Managing XenDesktop and NetScaler Agent instances	17
Configuring agent properties	21
Configuring XenDesktop Agent Base and OData Configuration properties	22
Configuring XenDesktop and NetScaler Agent Data Collection Scheduler properties ..	23
Configuring XenDesktop Agent Process Configuration properties	23
Configuring NetScaler Agent Configuration properties	24
Managing certificates for FglAM	24
Syntax Conventions	24
Managing certificates for SSL encryption	25
Managing Certificates for NetScaler Agent	26
Monitoring the performance of your XenDesktop environment	30
Exploring the XenDesktop Environment dashboard	31
Selecting monitored objects	31
Observing alarms	32
Activating Foglight for Citrix XenDesktop and XenApp licenses	33
Investigating the performance of XenDesktop infrastructure components	34
Exploring XenDesktop sites	38
Investigating the use of License Server, Delivery Controller, and Storefront resources	41
Exploring individual License Servers and Controllers	44
Monitoring Desktops	45
Investigating the use of Desktop resources	46
Monitoring Applications	51
Identifying top Application consumers	53
Investigating Application details	54
Monitoring Sessions	56
Observing the Session Overview	59
Investigating Session details (NetScaler data)	61
Investigating Session details (host data)	63
Exploring individual Sessions	65
Monitoring Users	87
Identifying top consumers	89
Investigating the levels of resource consumption	90
Monitoring Delivery Groups	92

Investigating Delivery Group details	94
Monitoring vSphere resources	95
Investigating the use of Virtual Center and ESX Host resources	98
Investigating the use of Datastore resources	101
Exploring individual Datastores	103
Viewing object dependencies	104
Using dependency maps	105
Exploring XenDesktop Alarms	107
Exploring alarm counts	107
Exploring the alarm table	108
Reviewing Frequently Asked Questions	109
Generating reports	110
About Us	112
Technical support resources	112

Getting started

Foglight® allows you to monitor Citrix® XenDesktop® and XenApp® environments. Foglight for Citrix XenDesktop and XenApp alerts you about infrastructure problems as soon as they develop, enabling you to resolve issues proactively before end users are affected. Early intervention ensures consistent application performance at established service levels. Foglight for Citrix XenDesktop and XenApp monitors the health of your virtual system by tracking the levels of resource utilization such as CPU, network, and memory consumption of individual objects in your integrated environment.

- [Before you begin](#)
- [Introducing the XenDesktop infrastructure](#)
- [Monitoring XenDesktop components](#)

Before you begin

- Ensure that Foglight for Citrix XenDesktop and XenApp is installed on the Management Server, and that you have a valid license. For more information, see the *Foglight for Citrix XenDesktop and XenApp Release Notes*.
- If you want to monitor a Virtual Center, you need a running instance of the VMware Performance Agent. This agent is provided with Foglight for VMware. For more information about this product, see the *Managing Virtualized Environments User and Reference Guide*.
- If you want to collect OS-level data from hosts in your XenDesktop environment, you need running instances of Foglight for Infrastructure Windows® or UNIX® agents. Foglight for Infrastructure monitors physical hosts and helps you analyze and prevent potential performance bottlenecks. Use it to understand the state of your system health, and to track the levels of resource utilization such as CPU, network, and memory consumption for individual objects in your integrated environment. For complete information, see your Foglight for Infrastructure documentation.
 - **NOTE:** To use HTTPs connection for XenDesktop agent in FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate of controller to the KeyStore of FglAM. For more information, see [Managing certificates for SSL encryption](#) on page 25.
 - **NOTE:** To use HTTPs connection for NetScaler agent in FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate of NetScaler to the JRE KeyStore of FglAM. For more information, see [Managing Certificates for NetScaler Agent](#) on page 26.

Introducing the XenDesktop infrastructure

Citrix® XenDesktop® is a virtualization solution that provides a complete virtual desktop experience to a wide variety of client devices.

Figure 1. XenDesktop Infrastructure



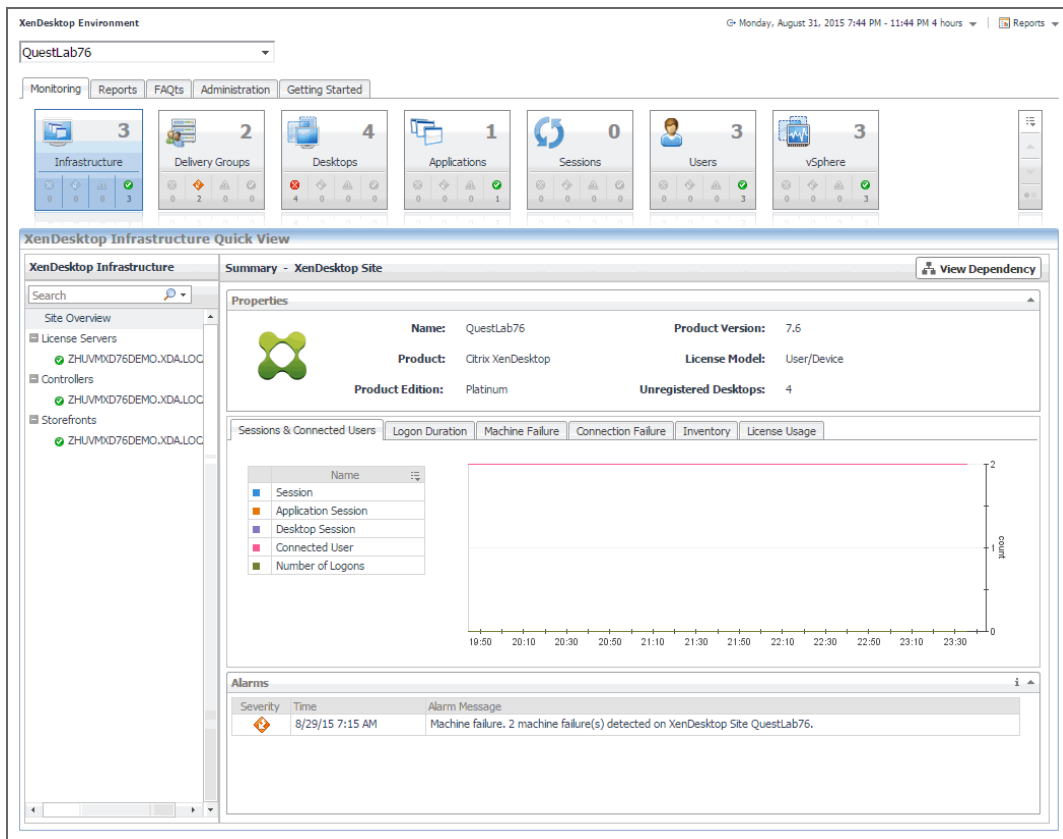
A typical XenDesktop environment consists of the following components:

- *Receiver*. A universal client application that runs on laptops and tablets.
- *NetScaler[®] gateway*. A WAN compression gateway that speeds up the delivery of desktop experience across slower networks. This is an optional component, but highly utilized.
- *XenDesktop Controller*. Manages user access to virtual applications and desktops, based on policies.
- *Desktops*. A desktop farm consisting of virtual machines and/or physical servers, that are served by the controller to end-users.
- *Director*. Present in all types of XenDesktop implementations, this component provides real-time monitoring information.
- *StoreFront*. Self-subscription service giving users convenient access to applications and desktops.

Monitoring XenDesktop components

Foglight for Citrix XenDesktop and XenApp allows you to monitor different components in your integrated XenDesktop[®] environment using the XenDesktop Environment dashboard. To access this dashboard, under **Dashboards**, click **XenDesktop**.

Figure 2. XenDesktop Environment dashboard



This dashboard focuses on the following components in your monitored XenDesktop environment:

- *XenDesktop Site* represents your monitored XenDesktop environment, consisting of Delivery Controllers, virtual desktops available for distribution to end-users, and other associated components.
- *License Servers* allow Citrix® licenses, including XenDesktop licenses, to be shared among application components.
- *Delivery Controllers* distribute virtual desktops to end-users, manage user access, and optimize connections.
- *StoreFronts* represent services that provide users with access to applications and desktops.

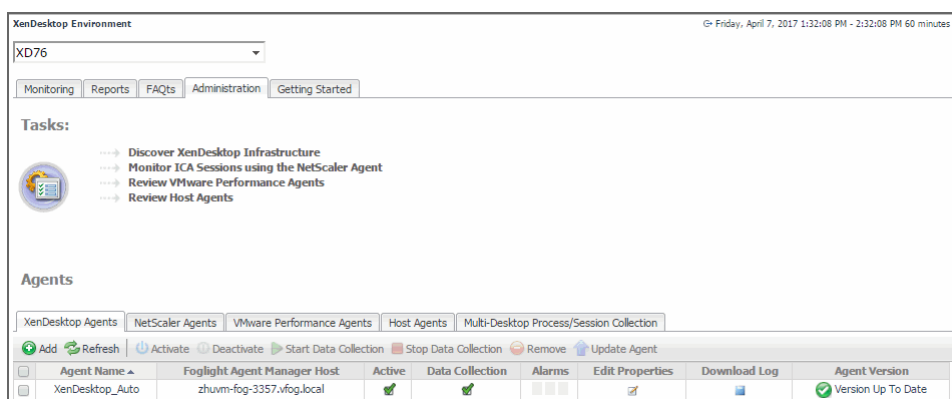
Setting up data collection agents

Foglight for Citrix XenDesktop and XenApp relies on XenDesktop and NetScaler Agents to collect data from the monitored system. When you install Foglight for Citrix XenDesktop and XenApp, you need to create appropriate agent instance to collect performance information from your environment.

Foglight for Citrix XenDesktop and XenApp includes a set of dashboards that allow you to monitor your XenDesktop® or XenApp® environment and manage monitoring agents. The XenDesktop Environment dashboard consists of several tabs, each focusing on a specific aspect of your monitoring needs.

The **Administration** tab allows you to create and manage monitoring agents. To access this tab, on the navigation panel, under **Dashboards**, choose **XenDesktop > XenDesktop Environment**, and then open the **Administration** tab.

Figure 3. Administration tab

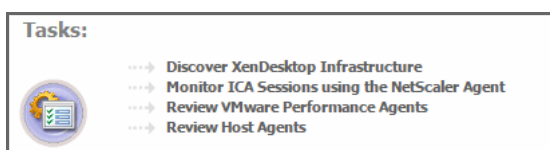


- [Exploring administration tasks](#)
- [Exploring and managing monitoring agents](#)
- [Configuring agent properties](#)

Exploring administration tasks

On the **Administration** tab, the **Tasks** area contains links to several administrative tasks that you can initiate from this tab.

Figure 4. Tasks area



- **Discover XenDesktop Infrastructure:** Run the **XenDesktop Discovery Wizard** to locate a XenDesktop® environment and create and configure a monitoring agent. This wizard automatically discovers your XenDesktop infrastructure, and creates the following agents:
 - XenDesktop Agent
 - VMware Performance Agents
 - Host Agents
 - Multi-Host Process Monitoring Agents

This is the first task you need to perform when working with Foglight for Citrix XenDesktop and XenApp. For more information, see [Discovering XenDesktop sites](#) on page 11.

- **Monitor ICA Sessions using the NetScaler Agent:** Run the **NetScaler Discovery Wizard** to locate a NetScaler® gateway and configure a monitoring agent. This task is only required if your XenDesktop environment has a NetScaler installer. For more information, see [Creating NetScaler Agent instances](#) on page 14.
- **Review VMware Performance Agents:** Review the list of monitored XenDesktop sites in the **Review VMware Agents** dialog box that appears when you click this link.

XenDesktop Site	Address	VMware Agent
vfogxda	zhuvmvfdvc.example.com	zhuvmvfdvc.example.com

If you have Foglight for VMware installed and deployed, for each XenDesktop site, the list displays the XenDesktop site name, the address of the associated virtual center, and the name of the VMware Performance agent that monitors the virtual center. If the virtual center is not currently monitored, but you have Foglight for VMware installed, you can create a VMware Performance agent by clicking the link in the **VMware Agent** column, and completing the steps in the **Agent Setup Wizard** that appears.

i TIP: Foglight for VMware allows you to monitor VMware virtual center by tracking resource consumption of individual physical and virtual elements in your integrated environment, and alerts you of issues that are likely to compromise your system stability. For more information, see your Foglight for VMware documentation.

- **Review Host Agents:** Review the list of the hosts associated with the monitored XenDesktop sites in the **Review Host Agents** dialog box that appears when you click this link.

Sites	Type	Host	Host Agent
NewSimulatorSite-1.2.1	Delivery Controller	SIMULATORCONTROLLERDNS	Create Host agent
	License Server	SIMULATORLICENSESERVER	Create Host agent
vfogxda	Delivery Controller License Server	ZHUVMVFOGCTRL.EXAMPLE.COM	Monitor@ZHUVMVFOGCTRL.EXAMPLE...
	Delivery Controller	ZHUVMVFOGCTRL2.EXAMPLE.COM	Create Host agent

If you have Foglight for Infrastructure installed and deployed, for each host in your XenDesktop environment, the list displays the associated XenDesktop site name, its type, the host name, and the name of the Foglight for Infrastructure Host agent that monitors that host. If the host is not currently monitored, but you have Foglight for Infrastructure installed, you can create a Host agent by clicking the link in the **Host Agent** column, and completing the steps in the **Add Monitored Host** wizard that appears.

i TIP: Foglight for Infrastructure monitors physical hosts and helps you analyze and prevent potential performance bottlenecks. Use it to understand the state of your system health, and to track the levels of resource utilization such as CPU, network, and memory consumption for individual objects in your integrated environment. For complete information, see your Foglight for Infrastructure documentation.

Discovering XenDesktop sites

A XenDesktop® environment contains one or more License Servers and delivery Controllers, and can be associated with a vCenter® server. Given a XenDesktop domain and host names, the **XenDesktop Discovery Wizard** allows you to locate these components and to create monitoring agents.

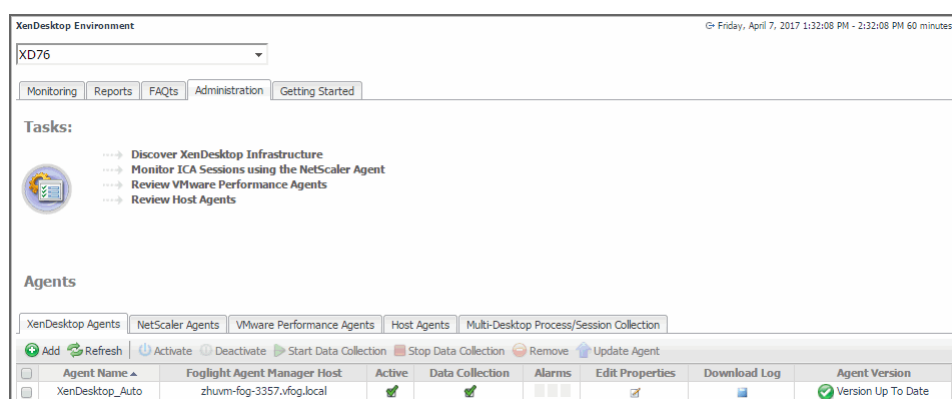
- NOTE:** Unlike the **Create XenDesktop Agent** wizard, the **Discover XenDesktop Wizard** offers to create VMware Performance agents for the detected vCenters, or Windows or Unix agents for the discovered servers, in addition to creating a XenDesktop Agent instance. For more information about the Create XenDesktop Agent wizard, see [Creating XenDesktop Agent instances](#) on page 20.

This results in two or more agent instances: a XenDesktop Agent (to monitor the XenDesktop server), one or more VMware Performance agents (to monitor the associated vCenters), and one or more Windows® or UNIX® agents (available with Foglight™ for Infrastructure, to monitor OS-level resources).

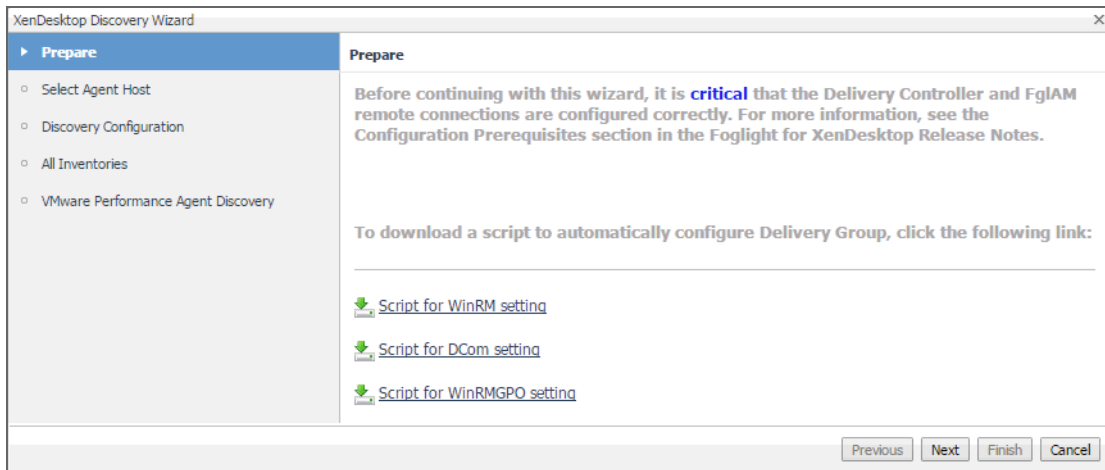
- NOTE:** The VMware Performance Agent is provided with Foglight for VMware. The Windows and Unix agents are provided with the Foglight for Infrastructure. Ensure these components are installed and enabled in your environment before running the **XenDesktop Discovery Wizard**. For complete information, see the Foglight for VMware and Foglight for Infrastructure documentation.

To start monitoring XenDesktop servers:

- 1 Log in to the Foglight browser interface.
- 2 On the navigation panel, under **Dashboards**, click **XenDesktop**.
- 3 Open the **Administration** tab.



- 4 Under **Tasks**, click **Discover XenDesktop Infrastructure** to launch the **XenDesktop Discovery Wizard**. The **XenDesktop Discovery Wizard** appears, showing the **Prepare** page. The page lists one or more hosts that are running Agent Manager instances.

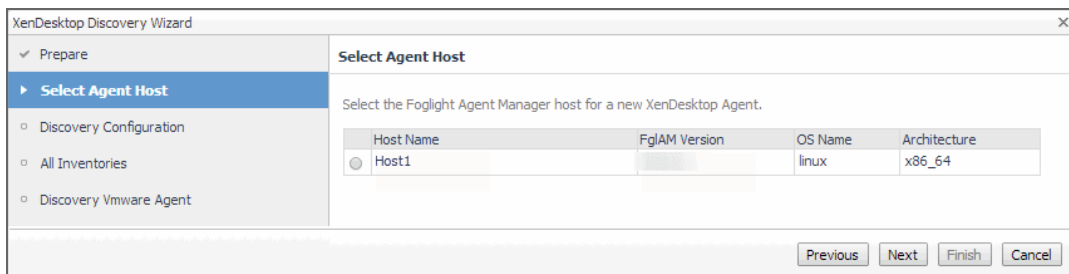


5 Review the information on the **Prepare** page.

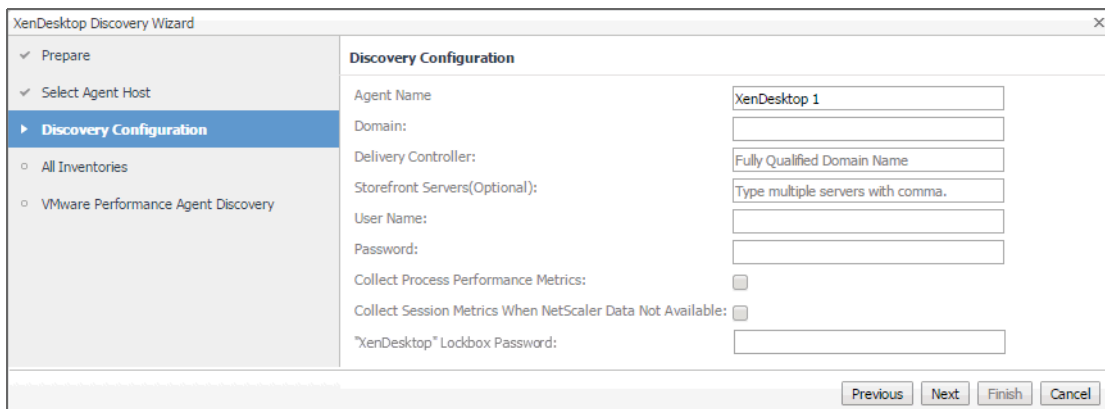
IMPORTANT: Before proceeding with this step, you must ensure that a WinRM or DCOM remote connection is enabled on the XenDesktop Delivery Controller node. Both WinRM and DCOM connections are supported, but WinRM is recommended.

- If you want to configure WinRM or DCOM settings automatically, click one of the following links to download the appropriate script:
 - **Script for WinRM setting**
 - **Script for DCom setting**
 - **Script for WinRM GPO setting**
- If you want to configure these settings manually, see the *Agent Manager Guide* for guidelines.

When done, click **Next**.



6 On the **Select Agent Host** page, select the running Agent Manager that you want to manage the monitoring agent that you are about to create, and click **Next**.



- 7 On the **Discovery Configuration** page, provide the following information needed to connect to the XenDesktop environment:
- **Agent Name:** Specify the name of the XenDesktop agent. If you want to specify a different name than the default name already provided (for example, `XenDesktop 1`), type it in this box.
 - **Domain:** Type the name of the domain to which the XenDesktop host belongs.
 - **Delivery Controller:** Type the name of the XenDesktop host. This value must include a fully qualified domain name.
 - **Storefront Servers (Optional):** Type a comma-separated list containing the names of StoreFront servers that provide access to desktops and applications. This step is optional.
 - **User Name:** Type the user name of the XenDesktop Delivery Controller login domain account (or the XenDesktop management account).
 - **Password:** Type the password associated with the above user name.
 - **Collect Process Performance Metrics:** Select this check box if you want the XenDesktop agent to collect virtual machine process metrics from the host.
 - **Collect Session metrics when NetScaler data not available:** Select this check box if you want the XenDesktop agent to collect session metrics when NetScaler data is not available. If you select this option and NetScaler data becomes available, the NetScaler data is displayed.
 - **XenDesktop Lockbox Password:** Type the password of the XenDesktop lockbox. This box only appears if your XenDesktop lockbox is protected with a password. This lockbox stores your XenDesktop credentials. For more information about credentials, see the *Administration and Configuration Help*.

When done, click **Next**.

- 8 On the **All Inventories** page, select one or more hosts that you want to monitor, and click **Next**.

- 9 On the **Discovery VMware Agent** page, the top table shows the vCenters that are not currently monitored. For each vCenter in that table, click the **Configure Agent** column to set up a VMware Performance agent for the vCenter.

The bottom table shows the monitored vCenters.

You can choose to set up your VMware Performance agents in this step, or later on using the **VMware Performance Agent** tab on the **Administration** tab of the XenDesktop Environment dashboard.

When done, click **Finish**.

The **XenDesktop Discovery Wizard** closes.

10 (Optional) Enable the IP mapping for the controller server, to set up the connection between storefront and delivery controller.

- a On the navigation panel, under Dashboards, click Administration > Agents > Agent Status.

The Agent Status dashboard opens.

- b Select an XenDesktop agent that you want to edit, click the Edit icon, and then click Edit Properties from the context menu.

The Edit Properties dialog box opens.

- c Click Modify properties for all XenDesktopAgent agents.

- d In the Delivery Controller IPs, multiple IPs with comma textbox, type the IP address of the delivery controller.

- e Click Save.

The Edit Properties dialog box refreshes and saves the IP address.

NOTE: In FIPS-compliant mode, you need to import the delivery controller certificate into FglAM. For more information, see [Managing certificates for SSL encryption](#) on page 25.

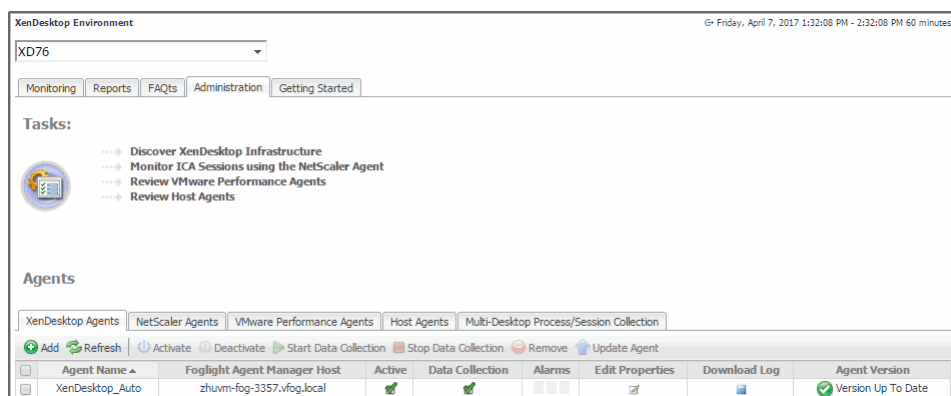
Creating NetScaler Agent instances

IMPORTANT: If your XenDesktop environment does not include NetScaler, you can disregard the information in this topic and skip this step.

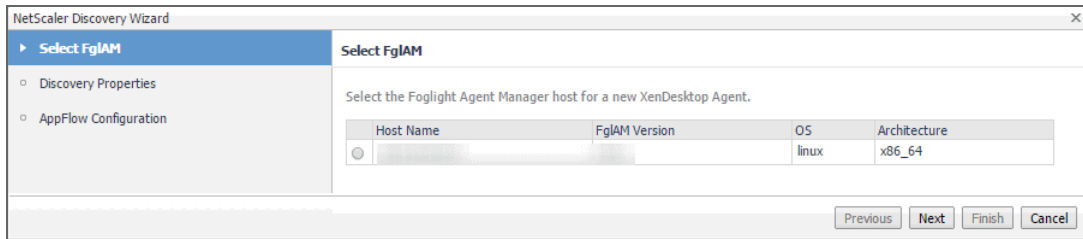
NetScaler Agents collect ICA (Independent Computing Architecture) session information from monitored Citrix® NetScaler® gateways using Citrix® AppFlow®. When the NetScaler Agent package is successfully deployed, you can create one or more NetScaler agent instances, activate them, and start their data collection. To perform these steps in a single operation, use the **NetScaler Discovery** wizard, accessible from the **Tasks** area on the **Administration** tab of the XenDesktop Environment dashboard.

To create and activate a NetScaler Agent instance, and start collecting data:

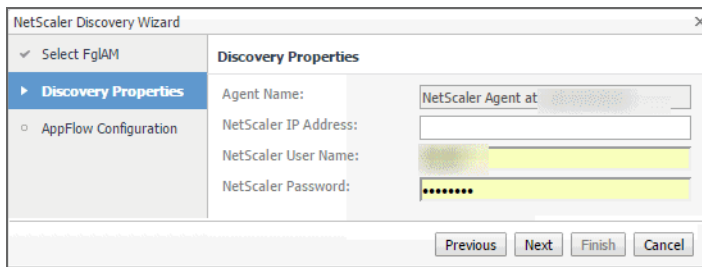
- 1 Log in to the Foglight™ browser interface.
- 2 On the navigation panel, under **Dashboards**, choose **XenDesktop > XenDesktop Environment**.
- 3 On the XenDesktop Environment dashboard that appears in the display area, open the **Administration** tab.



- In the **Tasks** area, click **Monitor ICA Sessions using the NetScaler Agent** to launch the **NetScaler Discovery Wizard**.

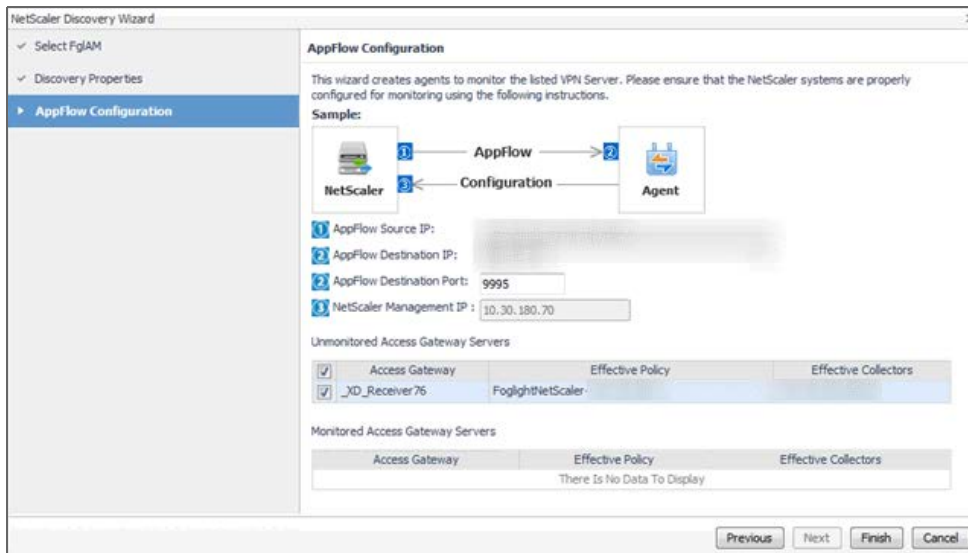


- In the **NetScaler Discovery Wizard**, on the **Select FglAM** page, select the host running the Agent Manager that you want to use to manage the agent instance you are about to create, and click **Next**.



- On the **Discovery Properties** page, provide the following information.
 - NetScaler IP Address:** The NetScaler IP address.
 - NetScaler User Name:** The user name required to access NetScaler.
 - NetScaler Password:** The password of the user account required to access NetScaler.

When done, click **Next**.



- On the **AppFlow Configuration** page, observe and configure the following parameters, as required. The NetScaler Agent needs this information to collect AppFlow data.
 - (1) AppFlow Source IP:** Shows the AppFlow Source IP that NetScaler uses to send NetFlow packets. The agent can handle multiple IPs automatically.
 - (2) AppFlow Destination IP, (2) AppFlow Destination Port:** Provide the IP address and port number the Agent Manager can use to receive AppFlow data sent by NetScaler.
 - (3) NetScaler Management IP:** Shows the NetScaler IP address.

- **Unmonitored Access Gateway Servers:** Select one or more NetScaler Gateway Servers that you want to monitor.

If you select a NetScaler Gateway Server that is already monitored by another agent, a message appears. You can either override the existing configuration, or clear your selection.

The Access Gateway(s) (_XD_Receiver76) was previously set up for Foglight monitoring. Selecting this gateway(s) will overwrite the existing configuration.

- **Monitored Access Gateway Servers:** If any NetScaler Gateway Servers are already monitored, they appear listed here.

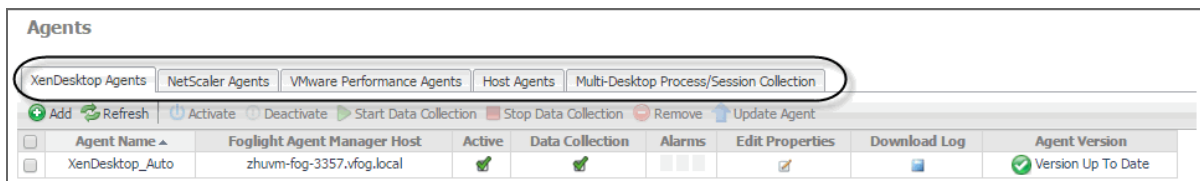
When done, click **Finish**.

- **NOTE:** To setup NetScaler agent in FIPS-compliant mode, you need to import NetScaler certification into FglAM default JRE. For more information, see [Managing Certificates for NetScaler Agent](#) on page 26.

Exploring and managing monitoring agents

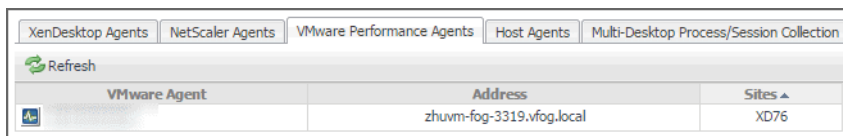
The **Agents** area contains several tabs that allow you to explore and manage the agent instances that monitor your integrated XenDesktop® environment. Each tab provides information about the agents of a specific type.

Figure 5. Agents tabs



- **XenDesktop Agents and NetScaler Agents tabs:** These tabs list the existing instances of the XenDesktop and NetScaler type, and allow you to manage them. These agents are provided with Foglight™ for Citrix XenDesktop and XenApp. For more information, see [Managing XenDesktop and NetScaler Agent instances](#) on page 17.
- **VMware Performance Agents tab:** This tab lists any existing VMware Performance Agent instances, provided with Foglight® for VMware, if you have Foglight for VMware installed and deployed.

- **TIP:** Foglight for VMware allows you to monitor VMware virtual centers by tracking resource consumption of individual physical and virtual elements in your integrated environment, and alerts you of issues that are likely to compromise your system stability. For more information, see your Foglight for VMware documentation.



For each VMware Performance Agent instance, the list displays its name, the address of the monitored virtual center, and the monitored XenDesktop site name.

- **Host Agents tab:** If you have Foglight for Infrastructure installed and deployed, this tab lists any existing Host Agent instances.

TIP: Foglight for Infrastructure monitors physical hosts and helps you analyze and prevent potential performance bottlenecks. Use it to understand the state of your system health, and to track the levels of resource utilization such as CPU, network, and memory consumption for individual objects in your integrated environment. For more information, see your Foglight for Infrastructure documentation.

Host Agent	Host	Type
Create Host agent	XD76CTRL1.VFOG.LOCAL	Delivery Controller(XD76)
Create Host agent	XD78-1.TCFNSF.VFOG.LOCAL	License Server(XD76)

The list displays the hosts in your XenDesktop environment, and for each monitored host it shows the name of the Host agent, the host name, and its type. If a host is not monitored, a link is provided to launch the **Add Monitored Host** wizard and create a Host Agent instance. For more information about this wizard, see your Foglight for Infrastructure documentation.

- **Multi-Desktop Process/Session Collection tab:** This tab lists XenDesktop sites.

Site	Process Collection	Session Collection	Desktops	Last Updated	Last Collection Duration
XD76	Enabled	Disabled	4	4/26/16 10:31 AM	0 ms

For each XenDesktop site, the list displays its name, the site name, indicates if the XenDesktop Agent monitors processes and sessions, the number of desktops, when it was last updated, and the duration of the most recent collection.

- To enable or disable the collection of process or session metrics for a site, click the **Process Collection** or **Session Collection** column, as required.
- To see which desktops are associated with a site, click the **Desktops** column.

Desktop	Active Sessions	Collected Processes	Last Updated
win7Static012.xda.local	0	3	4/26/16 3:52 AM
win7Static011.xda.local	0	0	4/26/16 3:52 AM
win7Static014.xda.local	0	0	4/26/16 3:52 AM
win7Static013.xda.local	1	2	4/26/16 3:54 AM
win2k8001.xda.local	0	0	4/26/16 3:52 AM

Managing XenDesktop and NetScaler Agent instances

The **XenDesktop Agents** and **NetScaler Agents** tabs list the existing agent instances of these agents and allow you to manage them. Each tab contains a set of columns that indicate various states of individual agent instances, along with several commands that you can issue to manage them. For example, to see if an agent instance is collecting data, look at the agent's **Data Collection** column. A green check mark in this column indicates that the agent is collecting data.

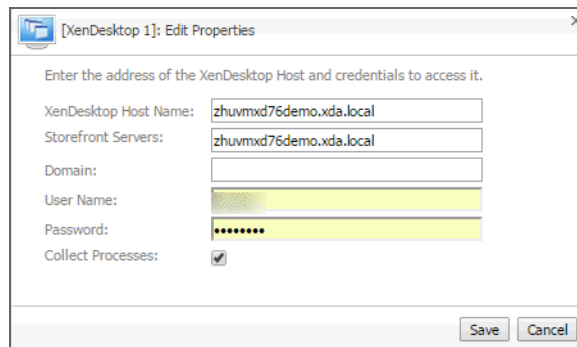
With the exception of the **Alarms** column that only appears on the XenDesktop Agents tab, the type of information appearing on these two tabs is identical.

Figure 6. XenDesktop Agents tab

XenDesktop Agents NetScaler Agents VMware Performance Agents Host Agents Multi-Host Process Monitoring Agents									
+ Add ↻ Refresh ⏸ Activate ⏹ Deactivate ▶ Start Data Collection ⏹ Stop Data Collection 🗑 Remove ↕ Update Agent									
Agent Name	Foglight Agent Manager Host	Active	Data Collection	Alarms	Edit Properties	Download Log	Agent Version		
XenDesktop.Dev		✔	✔	0	✎	📄	Update Agent		
XenDesktop.Simulator		✔	✔	0	✎	📄	Update Agent		

Table 1. XenDesktop Agents and NetScaler Agents tab contents

Agent Name	The name of the agent instance.
Foglight Agent Manager Host	The name of the machine on which the Agent Manager process is running.
Active	Indicates if the agent process is running.
Data Collection	Indicates if the agent is collecting data from the monitored environment.
Alarms	The total numbers of Warning, Critical, and Fatal alarms generated against the agent instance. NOTE: This column only appears on the XenDesktop Agents , but not on the NetScaler Agents tab.
Edit Properties	Click to make changes to the agent's properties, as required.



Edit one or more of the following properties, as required.

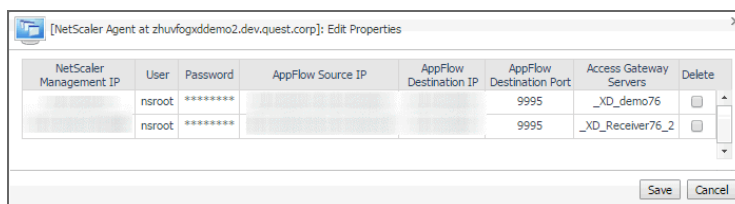
XenDesktop Agent

- **XenDesktop Domain:** The name of the domain to which the monitored XenDesktop® system belongs.

NOTE: The **XenDesktop Domain**, **User Name**, and **Password** boxes should only be populated if you need to change these values. Otherwise, they can remain clear.

- **Storefront Servers:** A comma-separated list containing the names of StoreFront servers that provide access to desktops and applications. This step is optional.
- **XenDesktop Host Name:** The name of the machine hosting the XenDesktop site.
- **User Name:** The user name the agent instance needs to connect to the XenDesktop site.
- **Password:** The password associated with the XenDesktop user.
- **Collect Processes:** Select this check box if you want the XenDesktop agent to collect process metrics.

Table 1. XenDesktop Agents and NetScaler Agents tab contents



Edit one or more of the following properties, as required.

NetScaler Agent

- **NetScaler Management IP:** The NetScaler IP address.
- **User:** The user name required to access NetScaler.
- **Password:** The password of the user account required to access NetScaler.
- **AppFlow Source IP:** A comma-separated list containing the AppFlow Source IP addresses that NetScaler uses to send NetFlow packets. The agent can handle multiple IPs automatically.
- **AppFlow Destination IP, AppFlow Destination Port:** The IP address and port number the Agent Manager can use to receive AppFlow data sent by NetScaler.
- **Access Gateway Servers:** The monitored NetScaler Gateway Server.
- **Delete:** Select this option if you no longer want to monitor this NetScaler Gateway Server.

Download Log Click to download the agent’s log file.

Agent Version Indicates if the agent is running the latest version of the agent package (Version Up To Date), or it needs to be updated ().

The toolbar appearing on top of the **Agents** table provides a set of commands that allow you to manage XenDesktop Agent instances. To issue any of the available commands, simply select one or more agent instances using the check boxes in the left-most column, and click the appropriate button on the tool bar. For example, to start an agent’s data collection, select a XenDesktop Agent instance and click **Start Data Collection**.

Figure 7. Agents table toolbar

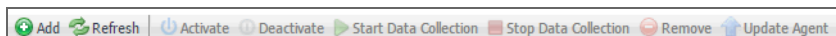


Table 2. Agents table toolbar

- Add** Launches a wizard that allows you to create a new agent instances:

 - **Create XenDesktop Agent** wizard starts from the **XenDesktop Agents** tab. For more information, see [Creating XenDesktop Agent instances](#) on page 20.
 - **NetScaler Discovery Wizard** starts from the **NetScaler Agents** tab. For more information, see [Creating NetScaler Agent instances](#) on page 14.
- Refresh** Refreshes the list of agent instances and their states.
- Activate** Activates the selected agent instances. Activating an agent instance starts the agent process on the machine on which the agent is installed.
- Deactivate** Deactivates the selected agent instances. Deactivating an agent stops the agent process on the machine on which the agent is installed.
- Start Data Collection** Starts the selected agent instances’ data collection. Starting an agent’s data collection causes the agent to begin monitoring the associated XenDesktop site and to send the collected metrics back to the Management Server.

Table 2. Agents table toolbar

Stop Data Collection	Stops the data collection of the selected agent instances. Stopping an agent's data collection causes the agent to stop monitoring the associated XenDesktop site.
Remove	Deletes the selected agent instances.
Update Agent	Updates the agent package to the latest version that is available on the Management Server.

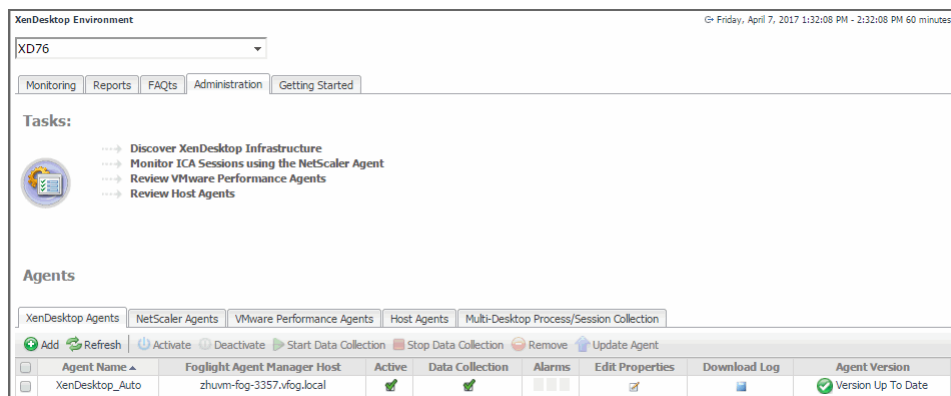
Creating XenDesktop Agent instances

XenDesktop Agents collect information from monitored hosts. When the XenDesktop Agent package is successfully deployed, you can create one or more agent instances, activate them, and start their data collection. To perform these steps in a single operation, use the **Create XenDesktop Agent** wizard, accessible from the **Agents** area on the **Administration** tab of the XenDesktop Environment dashboard.

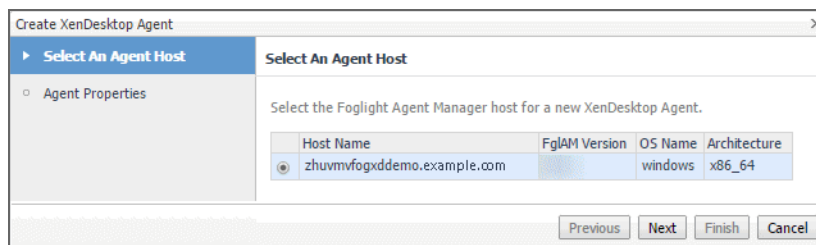
NOTE: Unlike the **Discover XenDesktop Wizard**, the **Create XenDesktop Agent** wizard does not offer to create VMware Performance agents for the detected vCenters, or to create Windows or Unix agents for the discovered servers. For more information about the **Discover XenDesktop Wizard**, see [Discovering XenDesktop sites](#) on page 11.

To create and activate a XenDesktop Agent instance, and start collecting data:

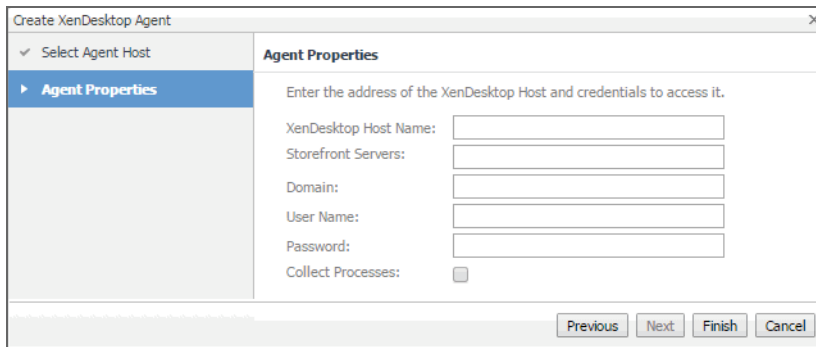
- 1 Log in to the Foglight browser interface.
- 2 On the navigation panel, under **Dashboards**, click **XenDesktop**.
- 3 On the XenDesktop Environment dashboard that appears in the display area, open the **Administration** tab.



- 4 In the **Agents** area, click **Add** to launch the **Create XenDesktop Agent** wizard.



- 5 Select the host running the Agent Manager that you want to use to manage the agent instance you are about to create, and click **Next**.



- 6 On the **Agent Properties** page, provide the following information.
 - **XenDesktop Domain:** The name of the domain to which the monitored XenDesktop® system belongs.
 - **Storefront Servers:** A comma-separated list containing the names of StoreFront servers that provide access to desktops and applications. This is optional.
 - **XenDesktop Host Name:** The name of the machine hosting the XenDesktop site.
 - **User Name:** The user name the agent instance needs to connect to the XenDesktop site.
 - **Password:** The password associated with the XenDesktop user.
 - **Collect Processes:** Select this check box if you want the XenDesktop agent to collect process metrics.
- 7 Click **Finish**.
The wizard closes, and the **Agents** area refreshes, showing a newly created agent instance.
- 8 Select the agent instance in the list and click **Activate**.
- 9 Click **Start Data Collection**.

Configuring agent properties

Foglight® uses the following agents to collect information from monitored environments:

- *XenDesktop Agent* collects information about your integrated XenDesktop® environment. For information about the XenDesktop Agent properties, see the following topics:
 - [Configuring XenDesktop Agent Base and OData Configuration properties](#) on page 22
 - [Configuring XenDesktop and NetScaler Agent Data Collection Scheduler properties](#) on page 23
- *NetScaler Agent* collects information about user experience data from monitored desktops, using AppFlow extensions. For information about the XenDesktopSession Agent properties, see the following topics:
 - [Configuring NetScaler Agent Configuration properties](#) on page 24
 - [Configuring XenDesktop and NetScaler Agent Data Collection Scheduler properties](#) on page 23

These agents collect data from the XenDesktop infrastructure and send it to the Management Server. They keep track of resource utilization metrics and alerts you when certain pre-defined thresholds are reached.

When an agent connects to vFoglight, it is provided with sets of properties that it uses to configure its correct running state. Each agent is provided with a combination of two types of properties: agent properties and shareable properties.

Default versions of these properties are installed with Foglight for Citrix XenDesktop and XenApp. However, you can edit the default shareable and agent properties, configure agent properties that apply only to a specific agent instance, and create edited clones of shareable properties that are used by a subset of agents of a certain type.

For detailed information about working with agent properties, see the *Administration and Configuration Help*.

To modify agent properties:

- 1 Log in to the Foglight browser interface.
- 2 Open the Agent Status dashboard and navigate to the agent properties.
 - a On the navigation panel, under **Dashboards**, choose **Administration > Agents > Agent Status**.
 - b On the Agent Status dashboard, select a XenDesktop or XenDesktop Session agent instance whose properties you want to modify, and click **Edit Properties**.
 - c Click **Modify the private properties for this agent**.
The agent properties appears in the display area.

Configuring XenDesktop Agent Base and OData Configuration properties

The XenDesktop Agent **Base Configuration** and **OData Configuration** properties specify general settings the agent needs to connect to the monitored environment.

Figure 8. Base Configuration and OData Configuration properties

Base Configuration	
Delivery Controller Hostname	<input type="text"/>
Delivery Controller IPs, multiple IPs with comma	<input type="text"/>
Collect Processes Performance Information	<input type="checkbox"/>
Collect Storefront Information	<input checked="" type="checkbox"/>
Storefront Hostnames	<input type="text"/>
Collect License Detail	<input checked="" type="checkbox"/>
Collect Session metrics from each desktop when NetScaler data not available	<input checked="" type="checkbox"/>

OData Configuration	
Is OData API using SSL.	<input type="checkbox"/>
OData API Port.	<input type="text" value="80"/>
Auto discover and Update OData API URL.	<input checked="" type="checkbox"/>

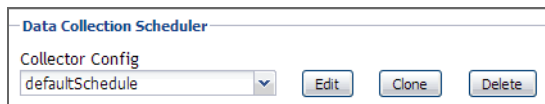
- **Base Configuration**
 - **Delivery Controller Hostname:** The name of the machine hosting the XenDesktop site.
 - **Delivery Controller IPs, multiple IPs with comma:** The IPs of the machine hosting the Xendesktop site.
 - **Collect Process Performance Information:** Indicates if the XenDesktop Agent collects process metrics. (Only WinRM connection is supported)
 - **Collect Storefront Information:** Indicates if the XenDesktop Agent collects StoreFront metrics.
 - **Storefront Hostnames:** A comma-separated list containing the names of StoreFront servers providing access to desktops and applications. This is optional.
 - **Collect License Detail:** Indicates if the XenDesktop Agent collects license-related information.
 - **Collect Session metrics from each desktop when NetScaler data not available:** Enable collect session metrics when not NetScaler data available. (Only WinRM connection is supported)
- **OData Configuration**
 - **Is OData API using SSL:** Indicates if the OData API, used by the XenDesktop Agent to access XenDesktop Controller's OData service, uses a secure internet connection.

- **OData API Port:** The port number the OData API uses for internet connections.
- **Auto discover and Update OData API URL:** Indicates if the OData API URL is automatically discovered and updated.

Configuring XenDesktop and NetScaler Agent Data Collection Scheduler properties

The **Data Collection Scheduled** properties allow you to adjust the frequency at which the XenDesktop or NetScaler Agent collects data from the monitored system.

Figure 9. Data Collection Scheduled properties

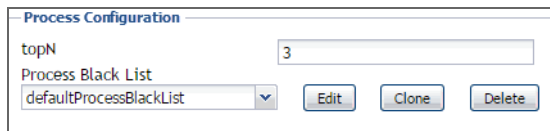


- **Collector Config:** A list identifying the data collectors the agent uses. Each entry in the list includes the following columns, allowing you to adjust the data collection settings for each individual collector:
 - **Collector Name:** The name of the collector: XenDesktop Data Collection.
 - **Default Collection Interval:** The length of the default collection interval.
 - **Time Unit:** The time unit for measuring the default collection interval: *milliseconds*, *seconds*, *minutes*, *hours*, or *days*.
 - **Fast-Mode Collection Interval:** The length of the collection interval when the agent is running in fast mode.
 - **Fast-Mode Time Unit:** The time unit of the collection interval when the agent is running in fast mode.
 - **Fast-Mode Max Count:** The maximum count of entries when the agent is running in fast mode.

Configuring XenDesktop Agent Process Configuration properties

The Process **Configuration** properties specify general settings the XenDesktop Agent needs to monitor session processes

Figure 10. Process Configuration properties

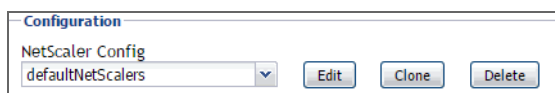


- **topN:** Instructs the XenDesktop Agents how many top processes to display on the XenDesktop Explorer **Processes** tab when a desktop session is selected.
- **Process Black List:** A list identifying the processes that you do not want to monitor. Each entry in the list includes the following column:
 - **Process Name:** The name of the process that you want to exclude from monitoring.

Configuring NetScaler Agent Configuration properties

The **Configuration** properties specify general settings the NetScaler Agent needs to connect to the NetScaler[®] gateway and to collect AppFlow[®] data.

Figure 11. Configuration properties



- **Automatic configure AppFlow Settings:** Indicates if the NetScaler Agent automatically configures AppFlow settings.
- **NetScaler Config:** A list identifying the monitored NetScaler gateways. Each entry in the list contains the following column:
 - **NetScaler's Ip:** The NetScaler IP address.
 - **Username:** The user name required to access NetScaler.
 - **Password:** The password of the user account required to access NetScaler.
 - **Sending IP:** The IP address from which NetScaler uses to send NetFlow packets.
 - **fglAM IP:** The IP address the Agent Manager uses to receive incoming data.
 - **VPN Servers:** Monitored NetScaler Gateway servers.

Managing certificates for FglAM

Refer to relevant sections for managing certificates for FglAM, according to your agent type:

- [Managing certificates for SSL encryption](#)
- [Managing Certificates for NetScaler Agent](#)

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 SSL encryption

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-----
```

i **NOTE:** If the certificate is not Base64 format, use openssl command to convert the certificate file into a Base64 file. Use either of the following commands depending on the source form:

```
openssl x509 -inform DER -in xxx.cer -out xxx.crt
or
openssl x509 -inform PEM -in xxx.cer -out xxx.crt
```

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

List installed certificates

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

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

Refer to the example output below:

```
List of installed certificates:

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

Delete a certificate

Remove a certificate referred to by an alias.

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

A full example for managing certificate for FglAM

- Add an example certificate into FglAM certificate store

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

...

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

- List the example certificate in the FglAM certificate store

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

...

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

- Delete the example certificate from the FglAM certificate store

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

...

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

Managing Certificates for NetScaler Agent

Back up custom JRE certificates before upgrading Agent Manager

When upgrading external Agent Manager, if the new Agent Manager uses a higher version JRE than the old Agent Manager, the JRE TrustStore (cacerts) in the old Agent Manager will be replaced by the new TrustStore from the higher version JRE. This will cause all the custom certificates imported to the old JRE TrustStore by customers get lost after the Agent Manager upgrade.

To keep the custom certificates, you need to back up the old JRE TrustStore before upgrading external Agent Manager, by following below steps:

- 1 Verify if the new Agent Manager uses a higher version JRE than the old Agent Manager.
- 2 If yes, copy the file <fglam_home>/jre/<current_jre_version>/jre/lib/security/cacerts to a local directory before upgrading Agent Manager.
- 3 After Agent Manager is upgraded, replace the cacert TrustStore with the copied cacert TrustStore and restart Agent Manager.

As for the embedded Agent Manager, it uses the same JRE as the Management Server. If there are custom JRE certificates stored in JRE TrustStore and a higher JRE version is used, back up the JRE cacert TrustStore used by the Management Server before upgrading Management Server.

i | NOTE: If the new JRE TrustStore has different entries than the old JRE TrustStore, there is a risk that these entries would get lost after replacing with the old JRE TrustStore.

Below is a list of JRE versions used by Agent Manager on various platforms in this release.

Platform	JRE Version
windows-x86_64	1.8.0.222
linux-x86_64	1.8.0.222
windows-ia32	1.8.0.181
linux-ia32	1.8.0.181
solaris-sparc64	1.8.0.181
solaris-x86_64	1.8.0.181
aix-powerpc64	1.8.0.537
hpux-ia64	1.8.0.18

Manage certificates for NetScaler agent in FIPS-compliant and non-FIPS mode

Add a certificate

- To add a certificate for an embedded FglAM, use the keytool command in FMS JRE located in `<foglight>/jre/bin`

```
keytool -import -trustcacerts -alias <alias> -file <Path  
To>/public_certificate.cer -keystore <foglight>/jre/lib/security/cacerts -  
storepass changeit
```
- To add a certificate for an external FglAM, use the keytool command in FglAM JRE located in `<fglam>/jre/bin`

```
keytool -import -trustcacerts -alias <alias> -file <Path  
To>/public_certificate.cer -keystore <fglam>/jre/lib/security/cacerts -  
storepass changeit
```
- 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-----
```

i NOTE: If the certificate is not Base64 format, use `openssl` command to convert the certificate file into a Base64 file. Use either of the following commands depending on the source form:

```
openssl x509 -inform DER -in xxx.cer -out xxx.crt  
or  
openssl x509 -inform PEM -in xxx.cer -out xxx.crt
```

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

List installed certificates

- Embedded FglAM:

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

- External FglAM:

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

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

Refer to the example output below:

```
Keystore type: jks
```

```
Keystore provider: SUN
```

```
Your keystore contains 149 entries
```

```
securetrustca [jdk], Dec 1, 2017, trustedCertEntry,
```

```
Certificate fingerprint (SHA1):
```

```
87:82:C6:C3:04:35:3B:CF:D2:96:92:D2:59:3E:7D:44:D9:34:FF:11
```

Delete a certificate

Remove a certificate referred to by an `alias`.

- Embedded FglAM:

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

- External FglAM:

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

A full example for managing certificate for NetScaler agent

- Embedded FglAM:

```
C:\Quest\Foglight\jre\bin> .\keytool.exe -import -trustcacerts -alias fveqaca
-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

- **External FglAM:**

```
C:\Quest\FglAM\jre\bin> .\keytool.exe -import -trustcacerts -alias fveqaca -  
file "C:\caca.cer" -keystore C:\Quest\FglAM\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

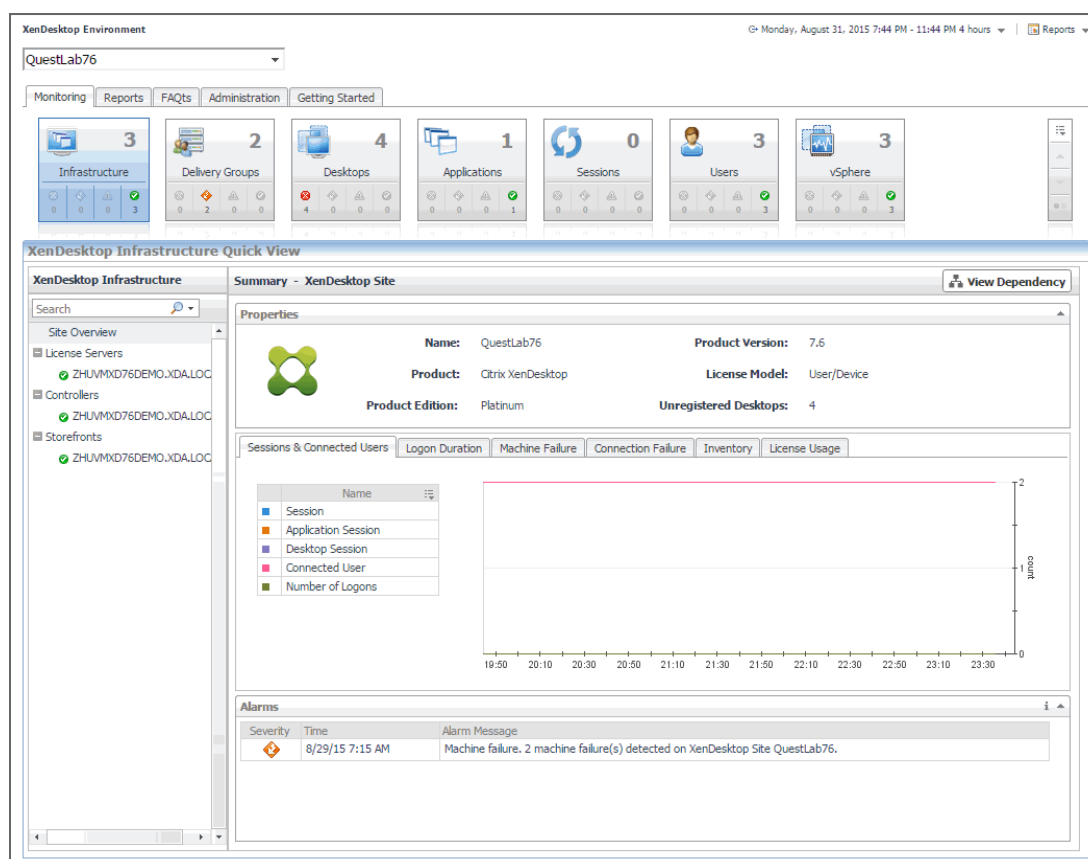
Certificate was added to keystore

Monitoring the performance of your XenDesktop environment

When you deploy Foglight for Citrix XenDesktop and XenApp and set up the monitoring agents for data collection, the XenDesktop Environment dashboard enables you to review the performance of your environment at a glance. Use this dashboard to ensure consistent application performance, by drilling down for details about individual components, to look for the indicators of performance degradation, such as high CPU load or network utilization.

A typical XenDesktop® environment contains a set of servers, delivery groups, desktops, and applications. You can view the overall state of these components on the XenDesktop Environment dashboard. To access this dashboard, under **Dashboards**, click **XenDesktop**.

Figure 12. XenDesktop Environment dashboard



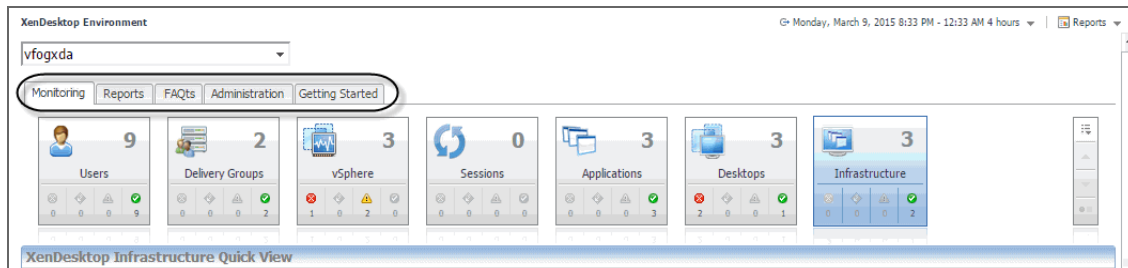
- Exploring the XenDesktop Environment dashboard
- Activating Foglight for Citrix XenDesktop and XenApp licenses
- Investigating the performance of XenDesktop infrastructure components
- Monitoring Desktops
- Monitoring Applications

- [Monitoring Sessions](#)
- [Monitoring Users](#)
- [Monitoring Delivery Groups](#)
- [Monitoring vSphere resources](#)
- [Viewing object dependencies](#)
- [Reviewing Frequently Asked Questions](#)
- [Generating reports](#)

Exploring the XenDesktop Environment dashboard

The XenDesktop Environment dashboard provides a set of tabs, each displaying a different aspect of your monitored system.

Figure 13. XenDesktop Environment tabs

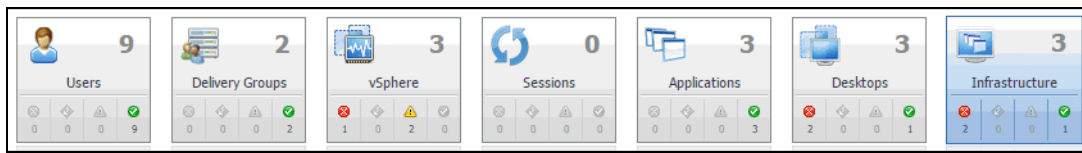


- **Monitoring:** Use this tab to review data specific to the main components of your monitored environment such as servers, delivery groups, desktops, applications, sessions, or vSphere resources. When you navigate to the XenDesktop Environment dashboard for the first time, the **Monitoring** tab appears open. This tab provides an overall summary of your monitored environment. It is described in this section.
- **Reports:** Use this tab to run and schedule Foglight for Citrix XenDesktop and XenApp reports. For more information, see [Generating reports](#) on page 110.
- **FAQs:** Use this tab to review the answers to common questions about your monitored systems. For more information, see [Reviewing Frequently Asked Questions](#) on page 109.
- **Administration:** Use this tab to discover XenDesktop® hosts, and to manage XenDesktop Agent instances. For more information, see [Setting up data collection agents](#) on page 9.
- **Getting Started:** Use this tab to activate, purchase, or renew your Foglight license. For more information, see [Activating Foglight for Citrix XenDesktop and XenApp licenses](#) on page 33.

Selecting monitored objects

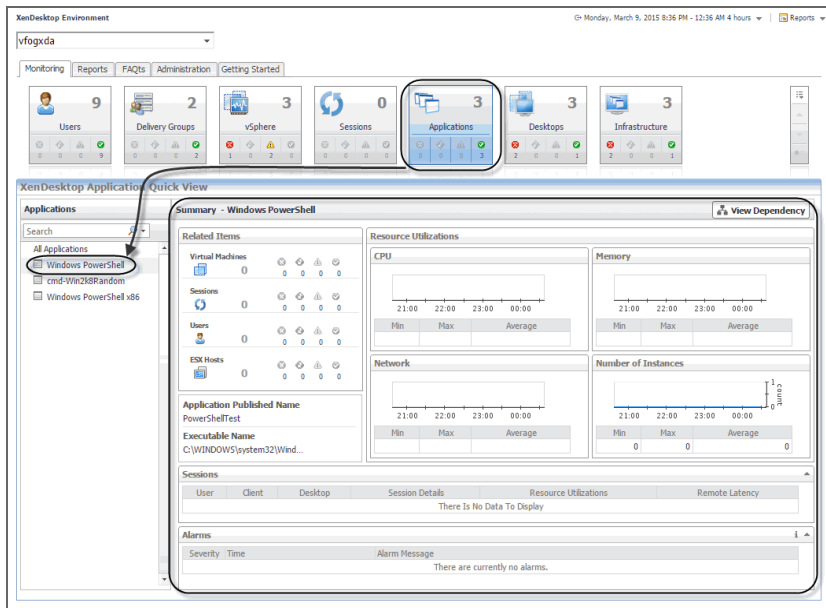
A set of tiles along the top of the **Monitoring** tab gives you a quick overview of the monitored objects: servers, delivery groups, desktops, applications, sessions, and vSphere® resources. Each tile represents a collection of a specific object type, shows the object count, and the count of objects in each alarm state (Normal, Warning, Critical, and Fatal).

Figure 14. Tiles representing monitored objects



The Quick View appearing immediately below the tiles allows you to select a specific instance of the tile selection. From here, you can drill down on a desired object instance, and review the related monitoring metrics.

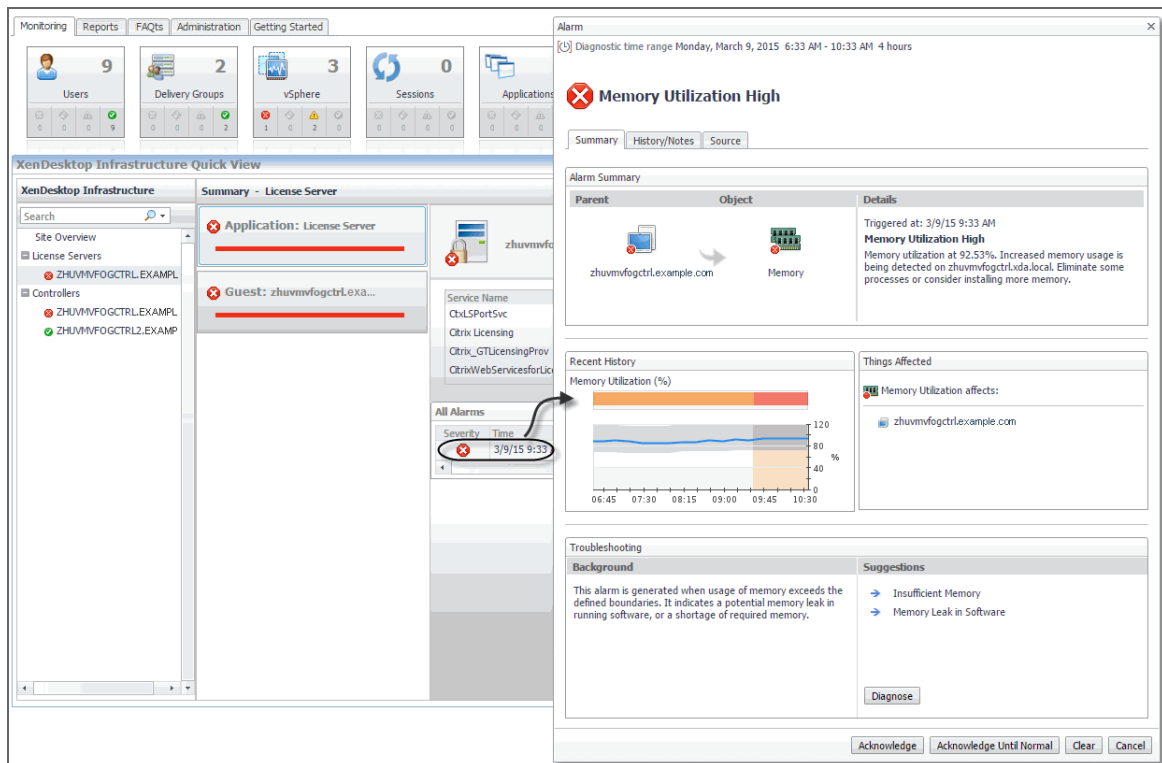
Figure 15. Drilling down on object in Quick View



Observing alarms

If any alarms are generated against certain types of monitored objects, they appear on the Monitoring tab, along the bottom of the summary view on the right. Drill down on an alarm to find out what triggered it, and to take steps to investigate further.

Figure 16. Drilling down on alarm



For complete information about alarms in Foglight™ for Citrix XenDesktop and XenApp, see the *Foglight for Citrix XenDesktop and XenApp User Guide*.

Activating Foglight for Citrix XenDesktop and XenApp licenses

Foglight for Citrix XenDesktop and XenApp is license-protected. When you install it for the first time, it comes with a 40-day trial license. You can activate it using the **Getting Started** tab. You can also use this tab to purchase or renew your Foglight for Citrix XenDesktop and XenApp license when your existing trial or commercial license expires. For more information, see the Foglight for Citrix XenDesktop and XenApp *Release Notes*.

Figure 17. Getting Started tab

Looking for VDI end-to-end Visibility?
Citrix XenDesktop and XenApp environment monitoring with Foglight™ for XenDesktop and XenApp.

Foglight™ for XenDesktop and XenApp alerts you about infrastructure problems as soon as they develop, enabling you to resolve issues pro-actively before end users are affected. Early intervention ensures consistent application performance at established service levels. Foglight™ for XenDesktop and XenApp monitors the health of your virtual system by tracking the levels of resource utilization such as CPU, network, and memory consumption of individual objects in your integrated environment.

Learn more about Foglight™ for XenDesktop and XenApp at <http://www.quest.com>

[Click Here to Activate a Free 30-Day Trial of Foglight for XenDesktop and XenApp](#)

Investigating the performance of XenDesktop infrastructure components

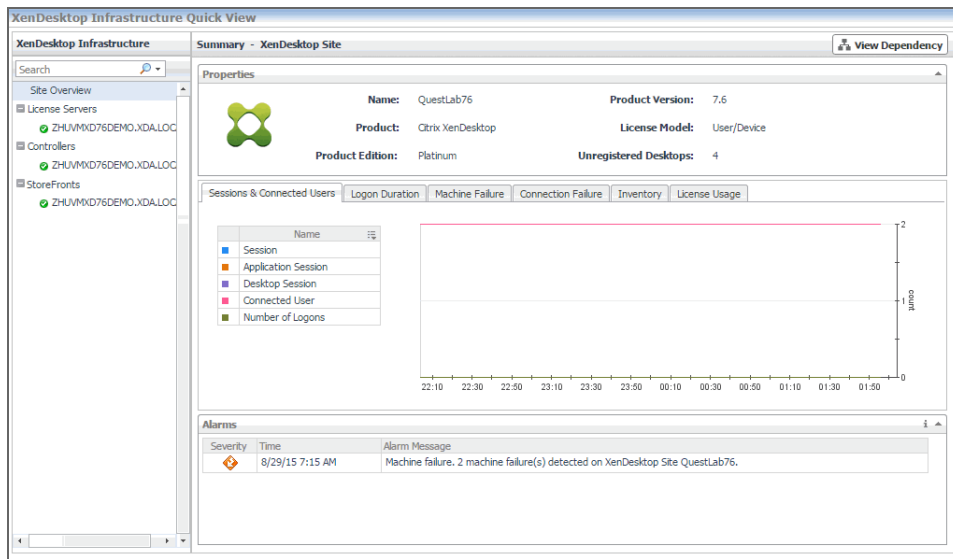
A typical XenDesktop® infrastructure consists the following high-level components:

- *XenDesktop Site* represents your monitored XenDesktop environment, consisting of Delivery Controllers, virtual desktops that they distribute to end-users, and other associated components.
- *Delivery Controllers* distribute virtual desktops to end-users, manage user access, and optimize connections.
- *License servers* allow Citrix® licenses to be shared among application components.
- *StoreFronts* represent services that provide users with access to applications and desktops.

You can monitor the performance of these components when you select the **XenDesktop Infrastructure** tile on the XenDesktop Environment dashboard.

The information appearing in the **XenDesktop Infrastructure Quick View** can help you discover potential resource-level issues such as spikes in session trends, and to reallocate resources where they are most needed.

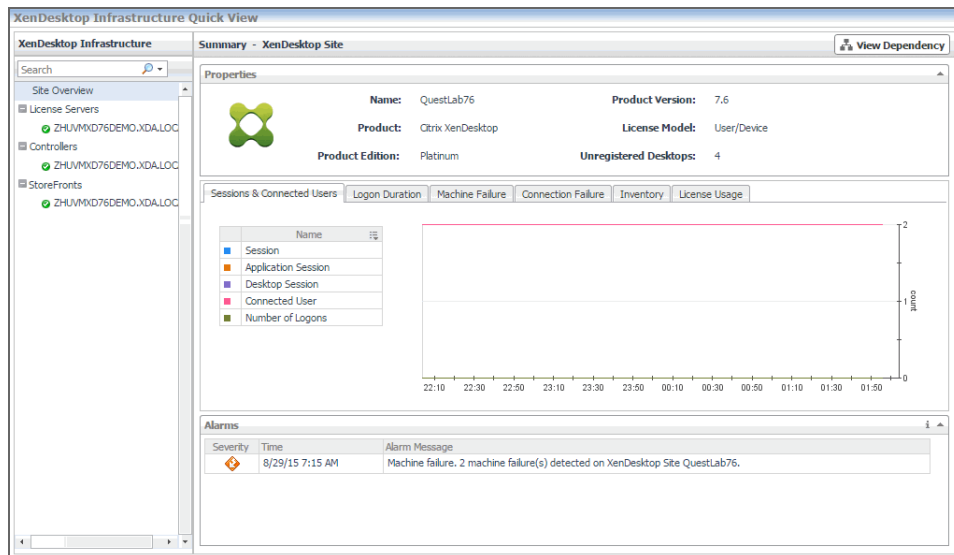
Figure 18. XenDesktop Infrastructure Quick View



To explore XenDesktop Sites, Delivery Controllers, and License Servers:

- 1 On the navigation panel, under **Dashboards**, click **XenDesktop Environment**.
- 2 On the XenDesktop Environment dashboard, on the **Monitoring** tab, click the **XenDesktop Infrastructure** tile.
- 3 In the **XenDesktop Infrastructure Quick View**, in the **XenDesktop Infrastructure** view on the left, click **Site Overview**.

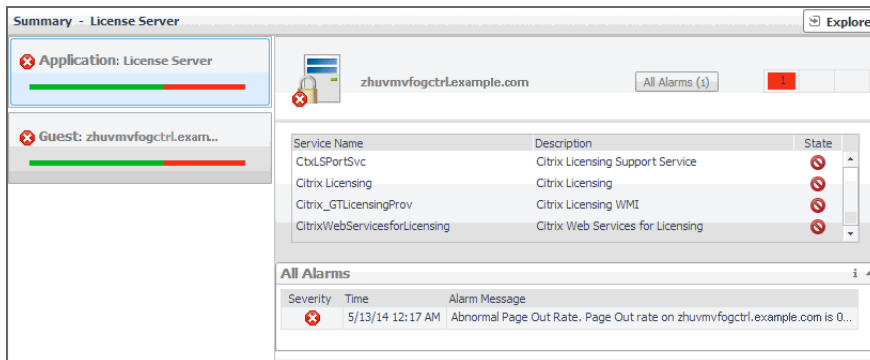
The **XenDesktop Infrastructure Quick View** refreshes, showing the **Summary - XenDesktop Site** view on the right.



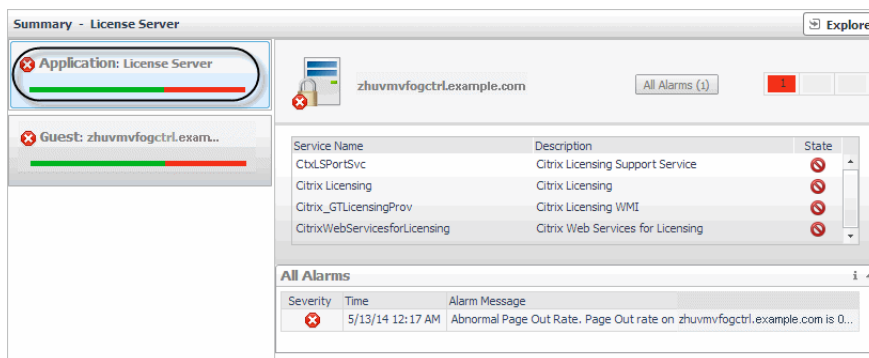
This view displays general information about the monitored XenDesktop site and shows the high-level performance trends in session counts, logon duration, machine and connection failures, and so on. For more information, see [Exploring XenDesktop sites](#) on page 38.

- 4 In the left pane, select a License Server, Delivery Controller, or Storefront.

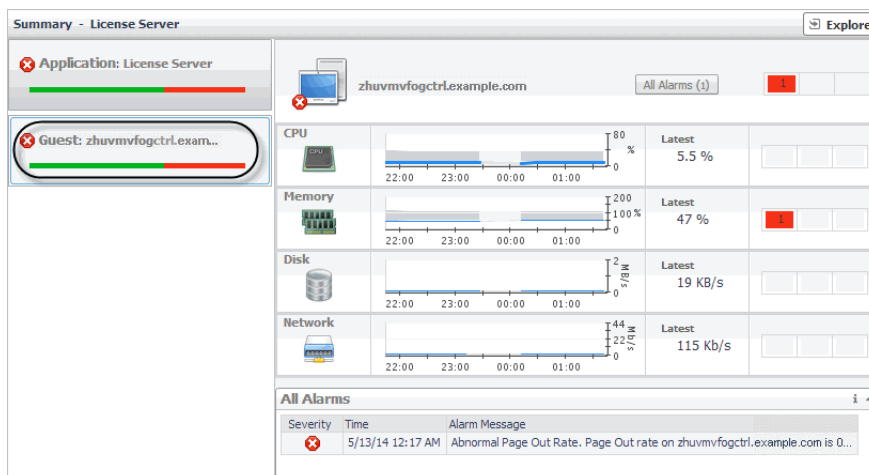
The **XenDesktop Infrastructure Quick View** refreshes, showing the summary information about the selected component on the right.



- When the **Application** tile on left is selected this view shows the list of services running on the selected License Server or Delivery Controller, and displays any alarms associated with it.



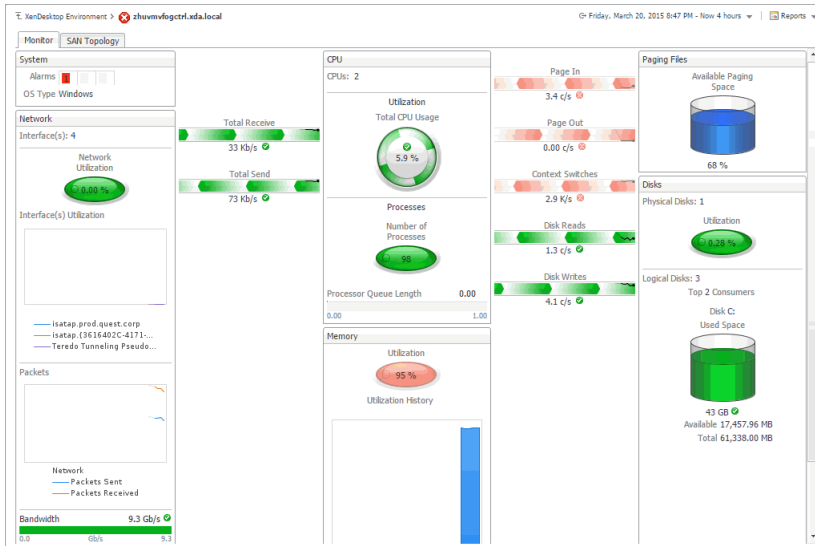
- When you select **Guest**, the view shows the usage of system resources on the machine on which the selected License Server or Delivery Controller is running.



For more information, see [Investigating the use of License Server, Delivery Controller, and Storefront resources](#) on page 41.

- Explore a License Server, Controller, or Storefront in more detail. In the top-right corner of the view, click **Explore**.

The display area refreshes.



The resulting view helps you understand the state of the resources of the host on which the License Server, Controller, or Storefront is running, if that host is already monitored with Foglight™ for Infrastructure. You can observe how the existing resource levels affect your monitored system as a whole. Along with displaying the system, network, CPU, memory, disk usage metrics, and any related alarms, this intuitive dashboard connects these visual elements with a series of graphical flows that illustrate how quickly the hosts transmits and processes data in real time. For example, you can review the rates of incoming and outgoing data and how they affect your network resources.

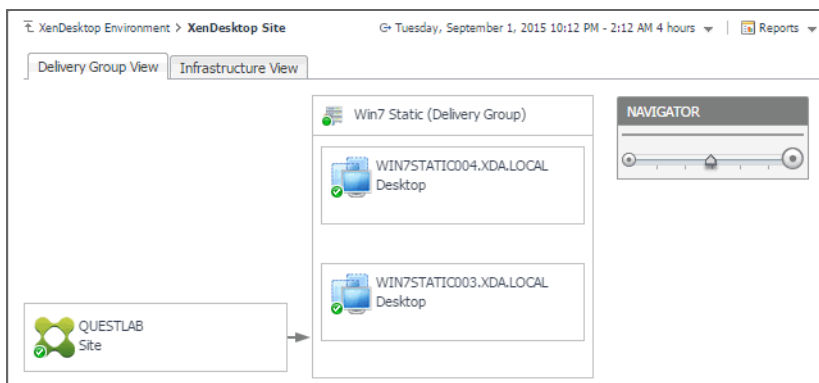
For more information, see [Exploring individual License Servers and Controllers](#) on page 44.

TIP: To return to the XenDesktop Environment dashboard, use the bread crumb trail in the top-left corner.

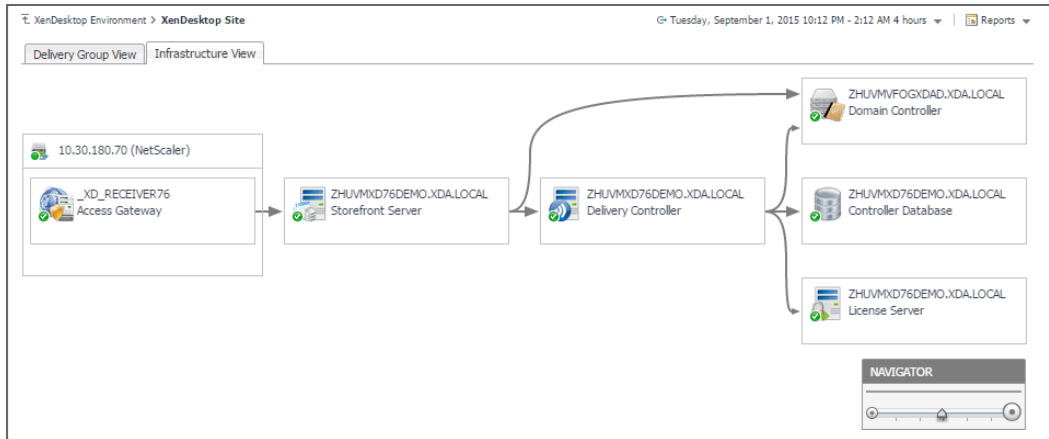
- 6 If you want to view the relationship your monitored XenDesktop site has with other components in your integrated environment, in the top-right corner, click **View Dependency**.

The display area refreshes, showing two tabs. Use the information appearing on these dependency maps to better understand the dependencies between the related components, and to look for any signs that may indicate potential performance degradation:

- **Delivery Group View:** A Delivery Group specifies which users can access Desktops or Applications based on their user type. This tab illustrates the relationships between main components associated with the Delivery Groups that belong to the selected XenDesktop site, including any Delivery Groups, Desktops, and Applications provided by the Delivery Groups.



- **Infrastructure View:** This tab illustrates the relationships between main infrastructure elements components associated with the Delivery Groups that belong to the selected XenDesktop site, such as the NetScaler Gateway, StoreFront Server, Delivery Controller, Domain Controller Database, and the License Server.



For more information about dependency maps, see [Viewing object dependencies](#) on page 104.

i | **TIP:** To return to the XenDesktop Environment dashboard, use the bread crumb trail in the top-left corner.

Exploring XenDesktop sites

A XenDesktop Site represents your monitored XenDesktop® environment, consisting of Delivery Controllers, virtual desktops, and other associated components. The **Summary - XenDesktop Site** view allows you to review general information about the monitored XenDesktop site along with performance trends in session counts, logon duration, machine and connection failures. Use this view to review the general trends in the overall performance of your monitored XenDesktop site and to look for any indicators that suggest potential bottlenecks. For example, an unusually high number of connection errors can affect the end-user experience and should be investigated.

Figure 19. Summary - XenDesktop Site view

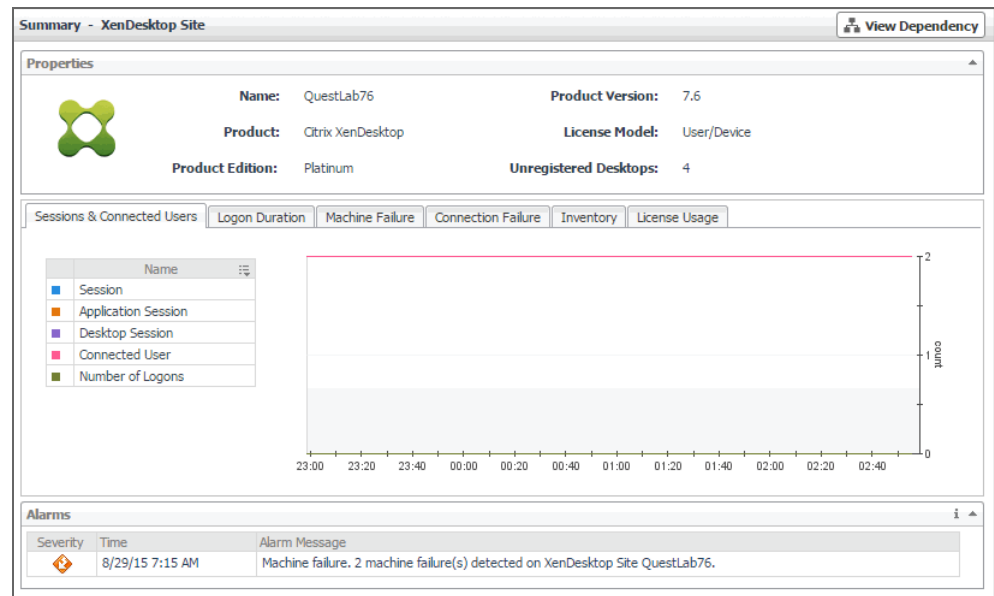


Table 3. Summary - XenDesktop Site view

Configuration details for the monitored XenDesktop Site: the name of the selected XenDesktop Site, the name of the XenDesktop application running on the monitored Site, the XenDesktop application edition, the XenDesktop version number, the type of the license model implemented at the monitored XenDesktop site, and the number of unregistered desktops. Citrix XenDesktop communicates with the controller in the monitored XenDesktop site using the Virtual Delivery Agent (VDA), and this state is referred to as being registered with the controller. A communication failure prevents XenDesktop to establish connection with the affected virtual desktops, causing them to turn into wasted resources. This information can help you troubleshoot problems related to an unsuccessful VDA registration.

Properties

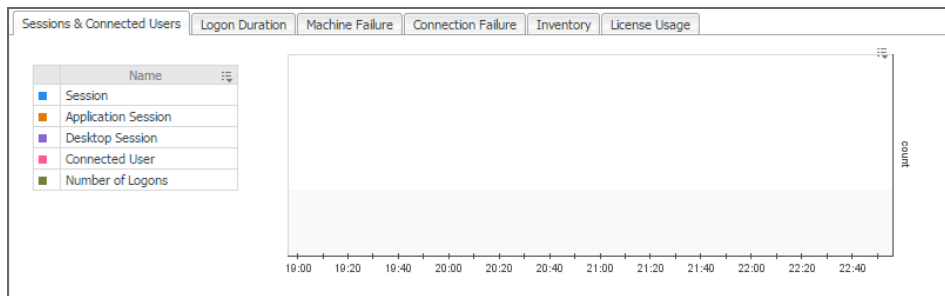
Name:	QuestLab76	Product Version:	7.6
Product:	Citrix XenDesktop	License Model:	User/Device
Product Edition:	Platinum	Unregistered Desktops:	4

Click **Unregistered Desktops** to find out the names and types (desktop, application, or desktop and application) of the unregistered desktops, and the delivery groups they belong to.

Delivery Group	Desktop	Desktop Type
Win7 Static Application	win7Static009.xda.local	AppsOnly
	win7Static010.xda.local	AppsOnly
win7StaticDesktop	win7Static008.xda.local	DesktopsOnly
	win7Static007.xda.local	DesktopsOnly

The session and user counts over the selected time period.

Session and Connected User



The logon duration times over the selected time period.

Logon Duration

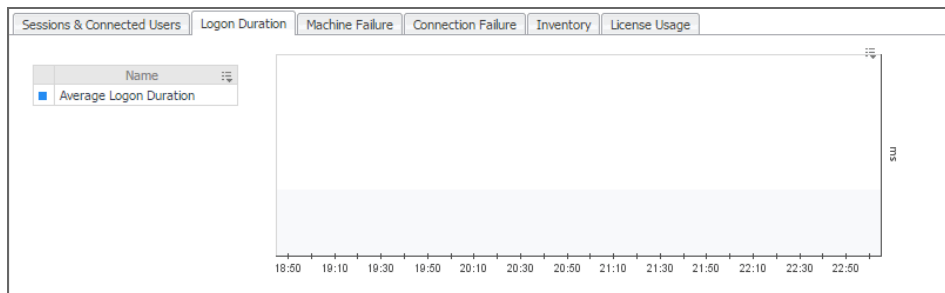
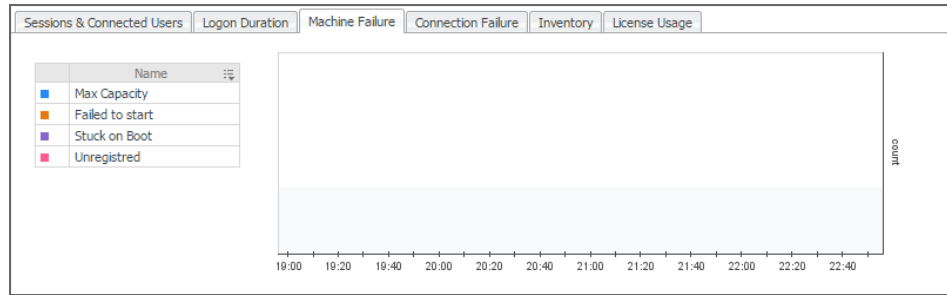


Table 3. Summary - XenDesktop Site view

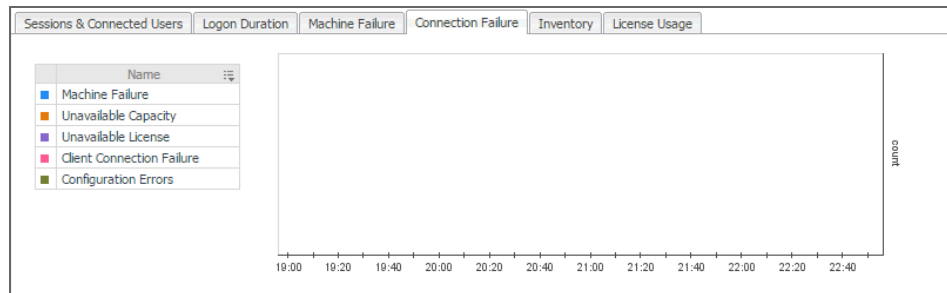
The counts of system-related failure types over the selected time period.

Machine Failure



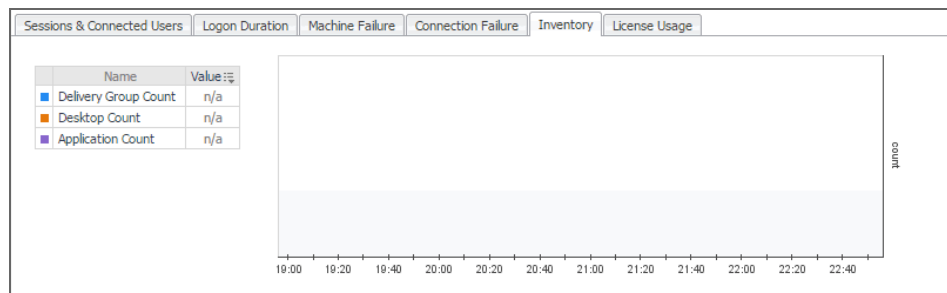
The counts of connection-related failure types over the selected time period.

Connection Failure



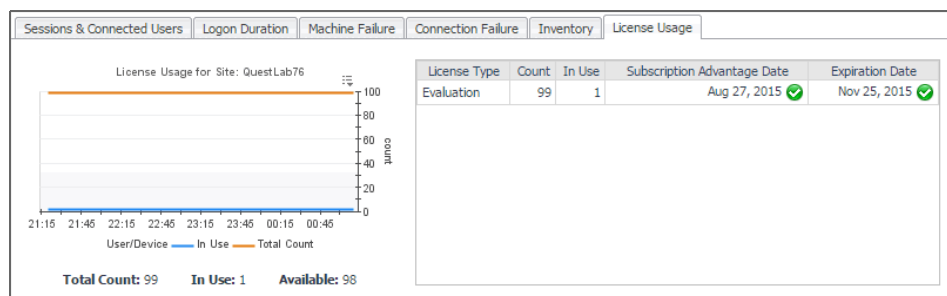
The counts of delivery groups, desktops, and applications over the selected time period.

Inventory



The counts of currently used licenses and available licenses over the selected time period. For each license type (for example, **Evaluation**), this view displays the total number of licenses, the number of used licenses, the dates when the licenses are first used, and their expiration date. Alarms are generated when the number of used licenses exceeds predefined thresholds.

License Usage



The alarms generated against the monitored XenDesktop Site. Each entry indicates the alarm severity (Warning, Critical, or Fatal), the time when the alarm was generated, and an explanation indicating what triggered the alarm.

Alarms

Severity	Time	Alarm Message
✖	5/13/14 12:17 AM	Abnormal Page Out Rate. Page Out rate on zhuvmvfogctrl.xda.local is 0.00.

Investigating the use of License Server, Delivery Controller, and Storefront resources

In your monitored environment, a Citrix License Server allows Citrix® licenses, including XenDesktop® licenses, to be shared among application components. Delivery Controllers distribute virtual desktops to end-users, manage user access, and optimize connections. Storefronts represent services that provide users with access to applications and desktops. You can review the performance of these components in the **Summary - License Server** and **Summary - Delivery Controller** views.

These views have two different layouts, depending on the tile selected on the left:

- [Application view](#)
- [Guest view](#)

Application view

Selecting the **Application** tile, the view shows the list of services running on the selected License Server, Controller, or Storefront, and displays any alarms associated with it. Use this view to see which services are running on the selected component, and to review any generated alarms, if they exist. For example, a high number of application-level alarms often suggest performance bottlenecks and should be investigated.

Figure 20. Application view

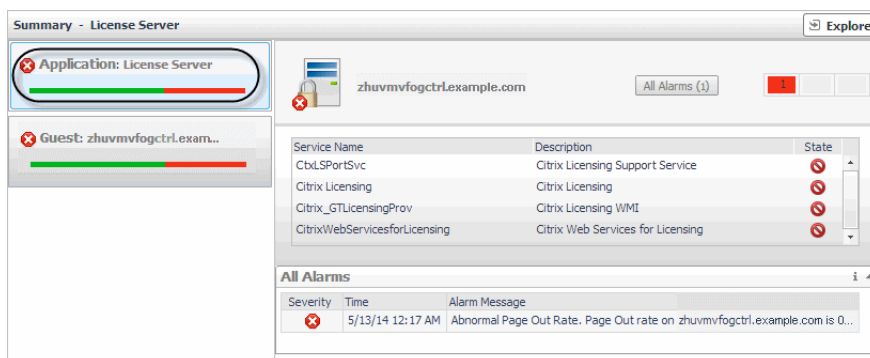


Table 4. Application view

The current alarm state of the selected component and its type (**License Server** or **Delivery Controller**). Selecting this tile displays the services associated with the selected component on the right.

Application

At the bottom of the tile, a color-coded health history bar indicates the alarm state of the selected component over the selected time range period. The color of the bar changes over that period depending on the alarm state. Red indicates that the selected component is in Fatal state, orange indicates Critical, yellow means Warning, and green is for the Normal state.

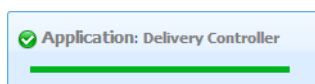


Table 4. Application view

A list of Citrix services running on the selected License Server or Delivery Controller, their description, and state.

Services

Service Name	Description	State
CitrixAdIdentityService	Citrix AD Identity Service	⊘
CitrixBrokerService	Citrix Broker Service	⊘
CitrixConfigurationService	Citrix Configuration Service	⊘
CitrixConfigurationLogging	Citrix Configuration Logging Service	⊘

Displays the alarms generated against the selected component (License Server or Delivery Controller). Each entry indicates the alarm severity (Warning, Critical, or Fatal), the time when the alarm was generated, and an explanation indicating what triggered the alarm.

All Alarms		
Severity	Time	Alarm Message
⊘	5/13/14 12:17 AM	Abnormal Page Out Rate. Page Out rate on zhuvmvfogctrl.example.com is 0...

Alarms

Clicking **All Alarms** just above the service table lists all alarms associated with the selected component. Optionally, you can drill down on a specific severity level (Warning, Critical, or Fatal) by clicking the appropriate box in the table on the right of **All Alarms**, to see only alarms with a specific severity level (for example, Warning alarms).



Guest view

When you select the **Guest** tile, the view shows the usage of system resources on the machine on which the selected License Server or Controller is running. Use this view to see the trends in usage of the selected component's system resources, and to review any generated alarms, if they exist. For example, high peaks in the memory utilization chart, that drastically exceed historical values could result in performance degradation and should be investigated.

Figure 21. Guest view

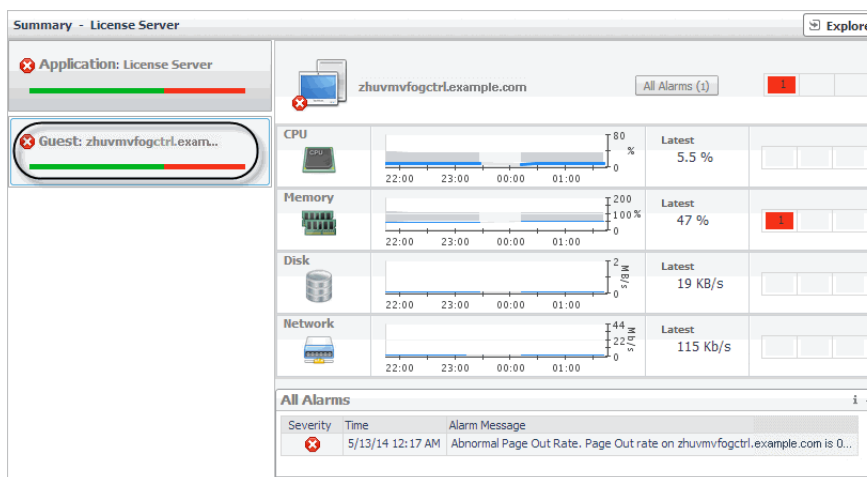
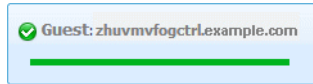
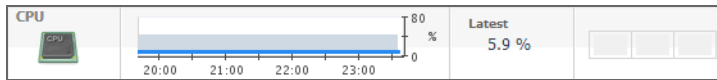


Table 5. Guest view

Guest The current alarm state of the selected component and its type (**License Server** or **Delivery Controller**). Selecting this tile displays the usage of system-level resources on the right. At the bottom of the tile, a color-coded health history bar indicates the alarm state of the selected component over the selected time range period. The color of the bar changes over that period depending on the alarm state. Red indicates that the selected component is in Fatal state, orange indicates Critical, yellow means Warning, and green is for the Normal state.

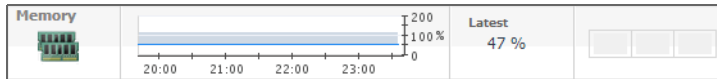


CPU The percentage of CPU resources the selected Delivery Controller or License Server consumed during the selected time range. The grey area in the chart represents the expected CPU utilization range based on historical data. The **Latest** percentage represents the current CPU utilization. If any CPU-related alarms are generated against the selected Delivery Controller or License Server, the counts of alarms in each severity state are displayed.



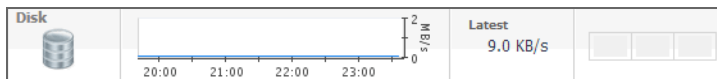
NOTE: Click an alarm severity to view a list all CPU-related alarms in that state in the [Alarms](#) view.

Memory The percentage of memory resources the selected Delivery Controller or License Server consumed during the selected time range. The grey area in the chart represents the expected memory utilization range based on historical data. The **Latest** percentage represents the current memory utilization. If any memory-related alarms are generated against the selected Delivery Controller or License Server, the alarm counts for individual severity states are displayed.



NOTE: Click an alarm severity to view a list all memory-related alarms in that state in the [Alarms](#) view.

Disk The rate at which the selected Delivery Controller or License Server writes to or reads from disk during the selected time range. The grey area in the chart represents the expected disk read and write rates based on historical data. The **Latest** rate represents the current disk rate. If any disk-related alarms are generated against the selected Delivery Controller or License Server, the alarm counts for individual severity states are displayed.



NOTE: Click an alarm severity to view a list all disk-related alarms in that state in the [Alarms](#) view.

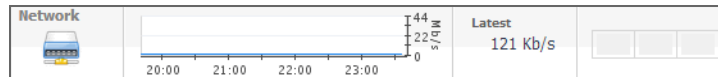
Table 5. Guest view

The rate at which the selected Delivery Controller or License Server transfers data from and to the network during the selected time range. The grey area in the chart represents the expected network transfer rates based on historical data.

The **Latest** rate represents the current network transfer rate.

Network

If any network-related alarms are generated against the selected Delivery Controller or License Server, the alarm counts for individual severity states are displayed.



NOTE: Click an alarm severity to view a list all network-related alarms in that state in the [Alarms](#) view.

Displays the alarms generated against the selected component (License Server or Delivery Controller). Each entry indicates the alarm severity (Warning, Critical, or Fatal), the time when the alarm was generated, and an explanation indicating what triggered the alarm.

Alarms

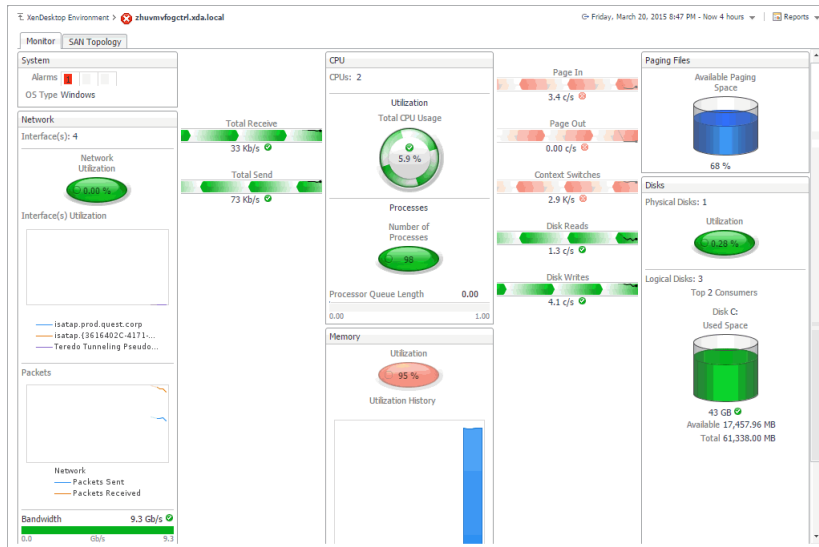
NOTE: Clicking **All Alarms** just above the service table lists all alarms associated with the selected component. Optionally, you can drill down on a specific severity level (Warning, Critical, or Fatal) by clicking the appropriate box in the table on the right of **All Alarms**, to see only alarms with a specific severity level (for example, Warning alarms).

Exploring individual License Servers and Controllers

If you see any indicators that can potentially lead to License Server or Delivery Controller performance degradation, you can explore these components in more detail to find out more information. The License Server and Delivery Controller Explorer views help you understand the state of the resources of the host on which the License Server or Deliver Controller is running, if that host is already monitored with Foglight™ for Infrastructure. You can observe how the existing resource levels affect your monitored system as a whole. Along with displaying the system, network, CPU, memory, disk usage metrics, and any related alarms, this intuitive dashboard connects these visual elements with a series of graphical flows that illustrate how quickly the hosts transmits and processes data in real time. For example, you can review the rates of incoming and outgoing data and how they affect your network resources. For complete information about this view, see your Foglight for Infrastructure documentation.

Use these views to look for any indicators that can help you understand the underlying cause of performance degradation. For example, a high number of alarms that indicate a shortage in system resources can be related to a problem leading to degradation in the overall end-user experience and should be further investigated.

Figure 22. Exploring License servers



Monitoring Desktops

A Desktop component in your monitored XenDesktop® environment encapsulates Windows® desktop and application components that are delivered to end-users on demand. You can monitor the performance of Desktop components when you select the **Desktops** tile on the XenDesktop Environment dashboard. The information appearing in the **XenDesktop Desktop Quick View** can help you discover potential resource-level issues such as spikes in resource utilization, and to reallocate resources where they are most needed.

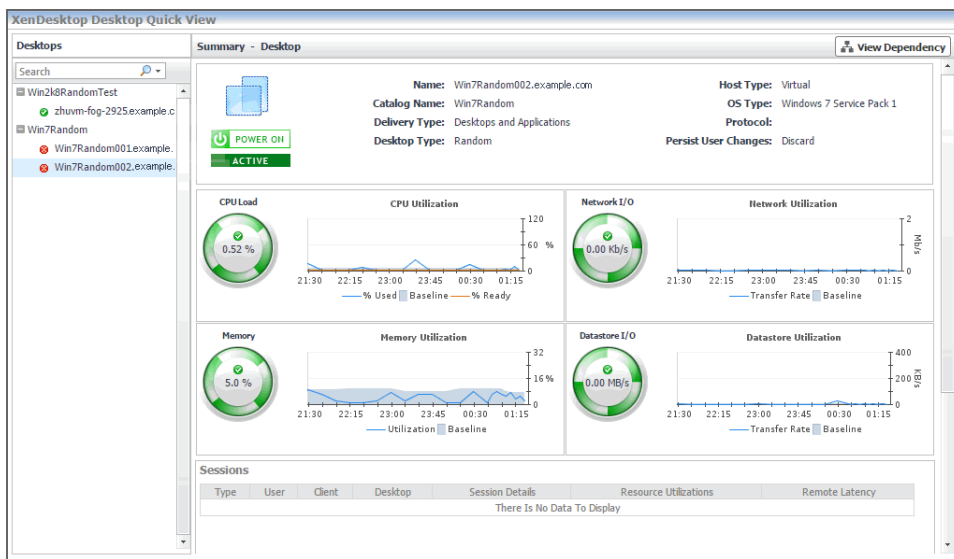
Figure 23. XenDesktop Desktop Quick View



To explore Desktops:

- 1 On the navigation panel, under **Dashboards**, click **XenDesktop Environment**.
- 2 On the XenDesktop Environment dashboard, on the **Monitoring** tab, click the **Desktops** tile.
- 3 In the **XenDesktop Desktop Quick View**, in the **Desktops** view on the left, click a desktop node.

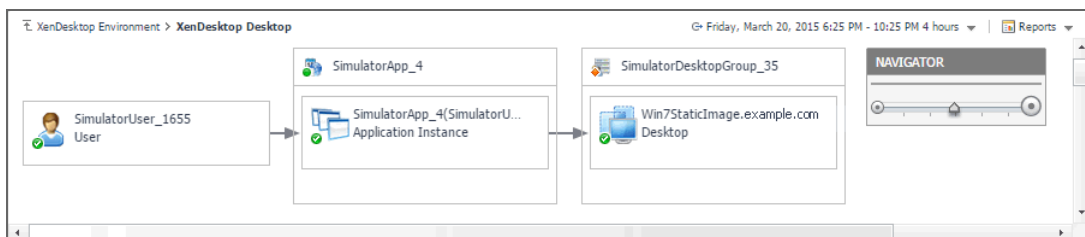
The XenDesktop Desktop Quick View refreshes, showing the **Summary - Desktop** view on the right.



This view displays general information about the selected desktop and shows the levels of resource utilization, and any alarms generated against the selected Desktop object, if they exist. For more information, see [Investigating the use of Desktop resources](#) on page 46.

- 4 If you want to view the relationship the selected Desktop object has with other components in your integrated environment, in the top-right corner, click **View Dependency**.

The display area refreshes, showing a dependency map.



The map illustrates how the selected Desktop object relates to other components in your monitored environment. For more information, see [Viewing object dependencies](#) on page 104.

TIP: To return to the XenDesktop Environment dashboard, use the bread crumb trail in the top-left corner.

Investigating the use of Desktop resources

In your monitored environment, a Desktop component encapsulates a Windows® desktop together with application elements that are delivered to end-users on demand. You can review the performance of individual desktops in the **Summary - Desktop** view. This view shows the usage of system resources for the selected desktop. Use it to see the trends in usage of the selected component's system resources, and to review any generated alarms, if they exist. For example, high peaks in the memory utilization chart, that drastically exceed historical values could result in performance degradation and should be investigated.

Figure 24. Summary - Desktop view

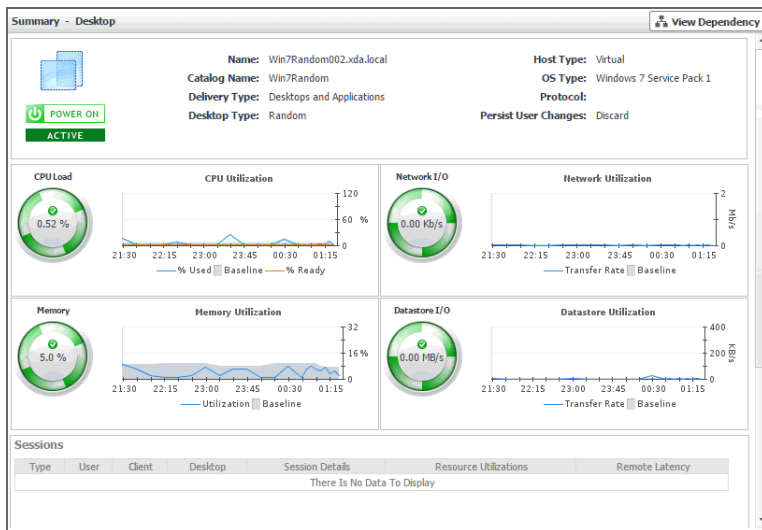





Table 6. Summary - Desktop view

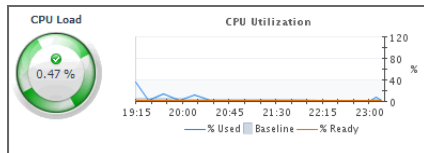
The configuration information about the selected desktop site: its name, the catalog name, whether it delivers desktops only or desktops with applications, whether it is a static or random desktop, whether it persists or discards user changes, whether it is a virtual or physical machine, the OS and protocol in use, and the host name and IP address (for physical hosts).

Desktop properties

  	Name: Win7Random002.example.com Catalog Name: Win7Random Delivery Type: Desktops and Applications Desktop Type: Random	Host Type: Virtual OS Type: Windows 7 Service Pack 1 Protocol: Persist User Changes: Discard
---	---	---

Depending on the type of selected desktop (physical or virtual), CPU metrics are displayed in two different views.

For virtual desktops, the **CPU** view displays the **CPU Load** spinner indicating the current percentage of the selected virtual machine's CPU load, used to execute system code and user programs, based on the total CPU capacity. The **% Used** line in the **CPU Utilization** chart shows the percentage of the CPU utilization used by the virtual machine to execute system code and user programs, during the selected time period. **% Ready** displays the percentage of the virtual machine's CPU resources that are ready to execute system code and user programs during the selected time period. The **Baseline** area in the chart indicates the expected CPU utilization range based on historical data.



CPU

For physical desktops, the **CPU Utilization** line in the chart shows the percentage of the CPU utilization used by the physical machine to execute system code and user programs, during the selected time period. **Run Queue Length** displays the number of processes that are waiting to be executed, during the selected time period. The **Baseline** area in the chart indicates the expected CPU utilization range based on historical data.

The **History** bar appearing above the chart indicates the alarm state of the selected desktop's CPU resources over the selected time range period. The color of the bar changes over that period depending on the alarm state. Red indicates that the selected component is in Fatal state, orange indicates Critical, yellow means Warning, and green is for the Normal state.

If any CPU-related alarms are generated against the desktop, the counts of alarms in each severity state are displayed.

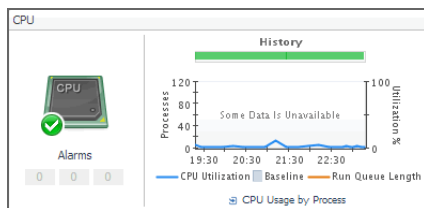
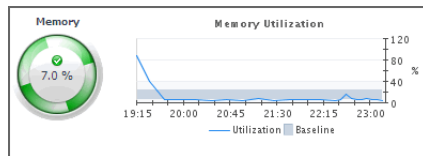


Table 6. Summary - Desktop view

Depending on the type of selected desktop (physical or virtual), memory metrics are displayed in two different views.

For virtual desktops, the **Memory** view displays the **Memory** spinner indicating the current percentage of the average memory usage by the selected virtual machine, based on the total memory capacity. The **Utilization** line in the **Memory Utilization** chart shows the percentage of memory used by the virtual machine during the selected time period. The **Baseline** area in the chart indicates the expected memory utilization range based on historical data.



Memory

For physical desktops, the **Memory Utilization** line in the chart shows the percentage of the memory resources physical machine uses during the selected time period. The **Baseline** area in the chart indicates the expected memory utilization range based on historical data.

The **History** bar appearing above the chart indicates the alarm state of the selected desktop's memory resources over the selected time range period. The color of the bar changes over that period depending on the alarm state. Red indicates that the selected component is in Fatal state, orange indicates Critical, yellow means Warning, and green is for the Normal state.

If any memory-related alarms are generated against the desktop, the counts of alarms in each severity state are displayed.

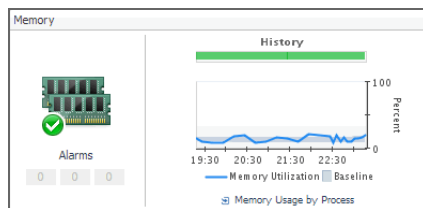
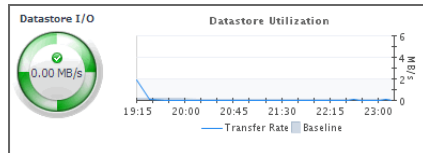


Table 6. Summary - Desktop view

Depending on the type of selected desktop (physical or virtual), disk storage metrics are displayed in two different views.

For virtual desktops, the **Datastore** view displays the **Datastore I/O** spinner indicating the current datastore I/O rate the selected virtual machine utilizes, based on the total datastore capacity. The **Transfer Rate** line in the **Datastore Utilization** chart shows the rate at which the virtual machine reads and writes data to the datastore during the selected time period. The **Baseline** area in the chart indicates the expected datastore utilization range based on historical data.



Datastore/Storage

For physical desktops, the **Disk Utilization** line in the chart shows the percentage of the disk resources the physical machine uses during the selected time period. The **Baseline** area in the chart indicates the expected disk utilization range based on historical data.

The **History** bar appearing above the chart indicates the alarm state of the selected desktop's disk resources over the selected time range period. The color of the bar changes over that period depending on the alarm state. Red indicates that the selected component is in Fatal state, orange indicates Critical, yellow means Warning, and green is for the Normal state.

If any memory-related alarms are generated against the desktop, the counts of alarms in each severity state are displayed.

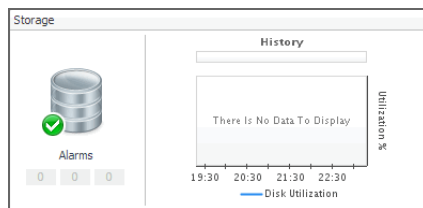
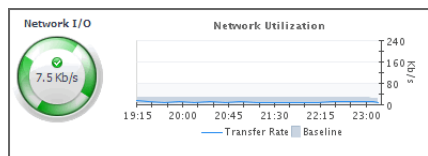


Table 6. Summary - Desktop view

Depending on the type of selected desktop (physical or virtual), network metrics are displayed in two different views.

For virtual desktops, the **Network** view displays the **Network I/O** spinner indicating the current rate at which the selected virtual machine transfers data from and to the network. The **Transfer Rate** line in the **Network Utilization** chart shows the rate at which the selected virtual machine receives and sends data to the network during the selected time period. The **Baseline** area in the chart indicates the expected network utilization range based on historical data.

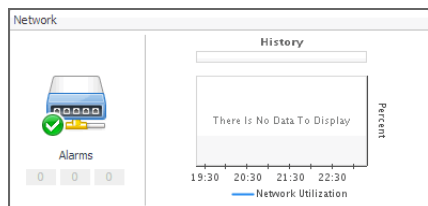


Network

For physical desktops, the **Network Utilization** line in the chart shows the percentage of the network resources the physical machine uses during the selected time period. The **Baseline** area in the chart indicates the expected disk utilization range based on historical data.

The **History** bar appearing above the chart indicates the alarm state of the selected desktop's network resources over the selected time range period. The color of the bar changes over that period depending on the alarm state. Red indicates that the selected component is in Fatal state, orange indicates Critical, yellow means Warning, and green is for the Normal state.

If any network-related alarms are generated against the desktop, the counts of alarms in each severity state are displayed.



General information about the session, such as its type (desktop or application), the user running the session, client name, desktop name, additional session details, resource utilization, and latency.

Sessions

Type	User	Client	Desktop	Session Details	Resource Utilization	Remote Latency	Explorer
Desktop	Caprice Juliana	Caprice_Juliana(10.0.0.9)	WIN7002.xda.local	View Session	View Details	View Details	Explorer

Alarms generated against the selected component (License Server or Delivery Controller). Each entry indicates the alarm severity (Warning, Critical, or Fatal), the time when the alarm was generated, and an explanation indicating what triggered the alarm.

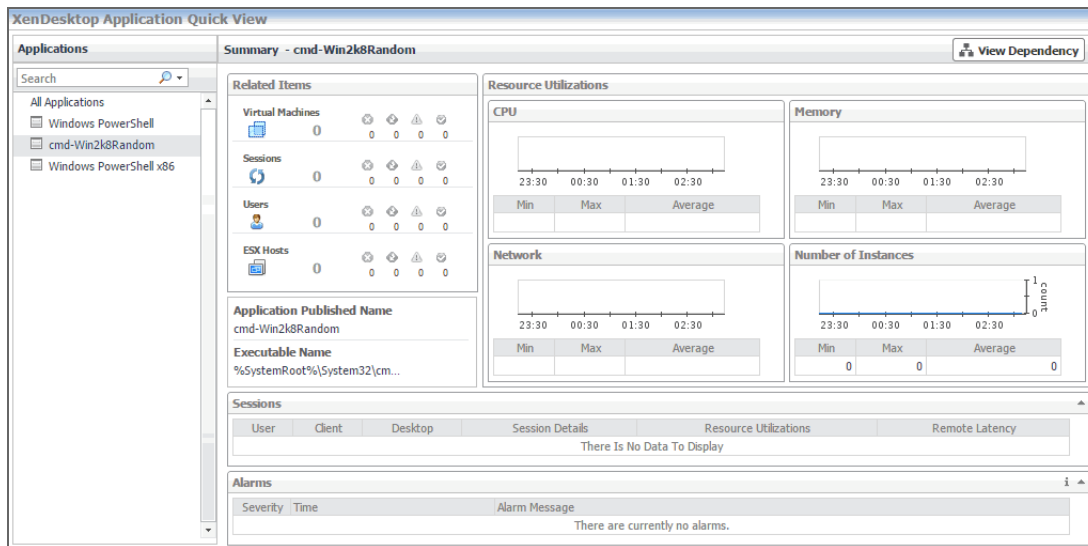
Alarms

Severity	Time	Alarm Message
Critical	4/23/14 9:54 AM	Swap Out Rate 157.01 B/s. Virtual machine Win08static02 is actively using memory that has been moved to the VMware swap fi

Monitoring Applications

XenDesktop® facilitates delivery of application components to end users on demand. You can monitor the performance of available applications when you select the **Applications** tile on the XenDesktop Environment dashboard. The information appearing in the **XenDesktop Application Quick View** can help you discover potential resource-level issues such as high number of application instances, and to reallocate resources where they are most needed.

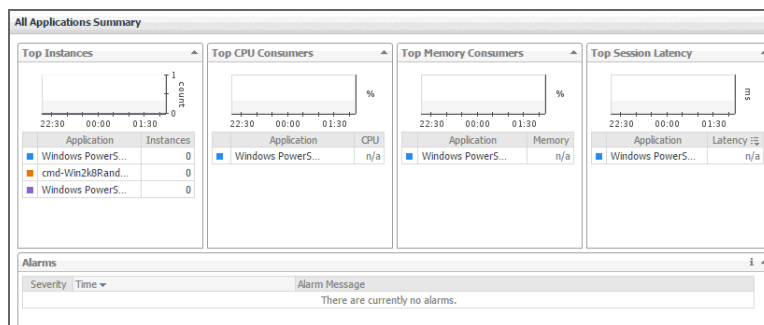
Figure 25. XenDesktop Application Quick View



To explore Applications:

- 1 On the navigation panel, under **Dashboards**, click **XenDesktop Environment**.
- 2 On the XenDesktop Environment dashboard, on the **Monitoring** tab, click the **Applications** tile.
- 3 In the **XenDesktop Application Quick View**, in the **Applications** view on the left, click **All Applications**.

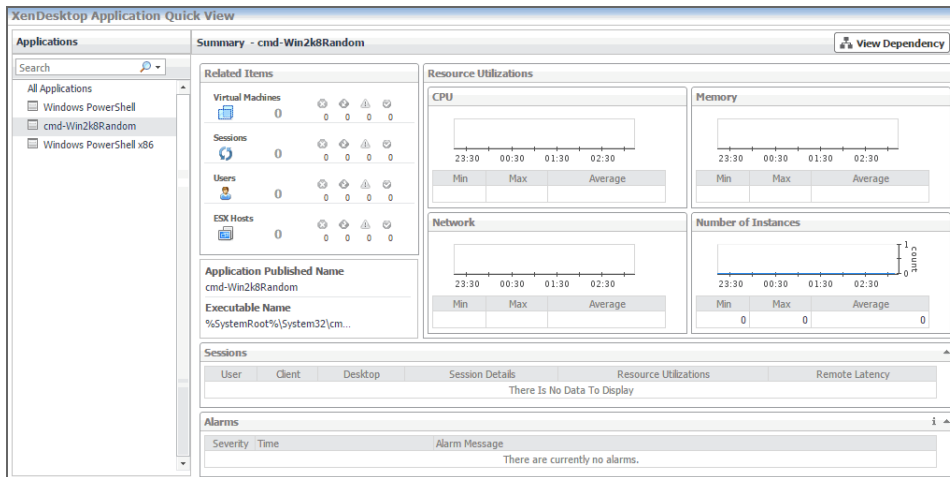
The **XenDesktop Application Quick View** refreshes, showing the **All Applications Summary** view on the right.



This view identifies the applications with the highest number of instances, and the highest CPU and memory utilization, and session latency. For more information, see [Investigating Application details](#) on page 54.

- 4 In the **XenDesktop Application Quick View**, in the **Applications** view on the left, click an application node.

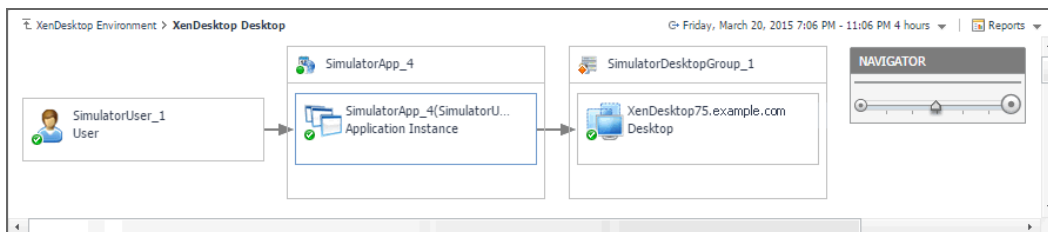
The **XenDesktop Application Quick View** refreshes, showing the **Summary - Application** view on the right.



This view displays general information about the selected application and shows the number of application instances that the end users are currently running. It also displays the levels of resource utilization for the selected application. For more information, see [Investigating Application details](#) on page 54.

- 5 If you want to view the relationship the selected Application object has with other components in your integrated environment, in the top-right corner, click **View Dependency**.

The display area refreshes, showing a dependency map.



The map illustrates how the selected Desktop object relates to other components in your monitored environment. For more information, see [Viewing object dependencies](#) on page 104.

i | TIP: To return to the XenDesktop Environment dashboard, use the bread crumb trail in the top-left corner.

Identifying top Application consumers

Your monitored XenDesktop environment delivers applications to end users on demand. The **All Applications Summary** view identifies the applications with the highest number of instances, and the highest CPU and memory utilization, and session latency. This view appears in the Quick View when you select **All Applications** in the **Applications** view on the left. Use it to look for potential bottlenecks in your system and prevent potential service disruptions by reallocating system resources where they are most needed.

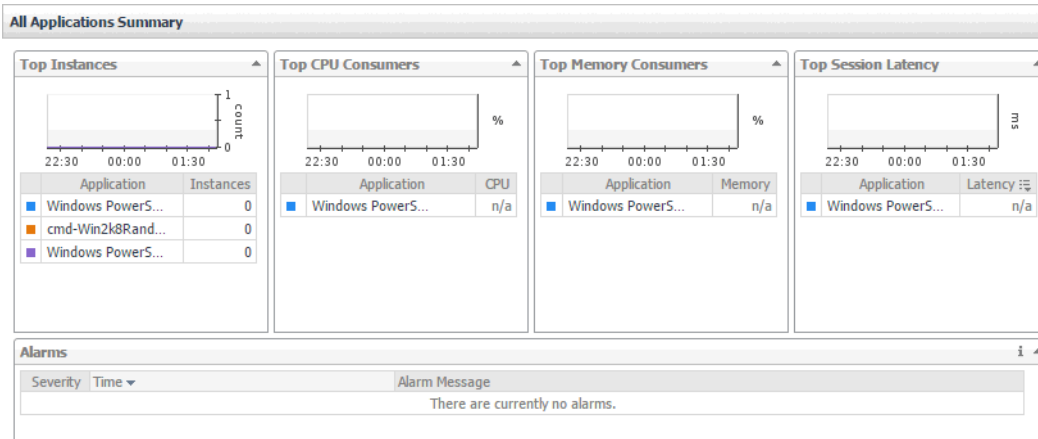
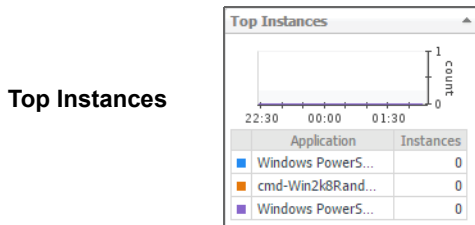
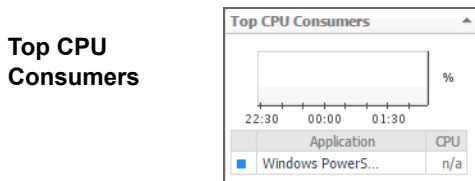


Table 7. Summary - Application view

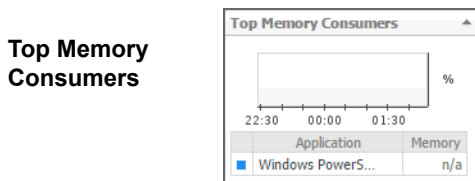
The applications with the highest number of running instances over the selected time range.



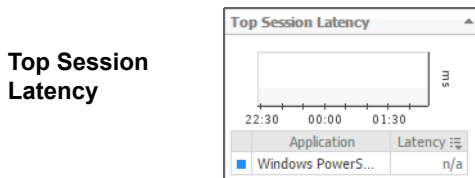
The applications consuming the highest amounts of CPU resources over the selected time range.



The applications consuming the highest amounts of memory resources over the selected time range.



The applications with the highest latency over the selected time range.



Investigating Application details

In your monitored environment, applications are delivered to end users on demand. You can review how individual applications are distributed to end users in the **Summary - Application** view. This view shows the usage of

system resources for the selected Application. Use it to see the number of users that are using it, and to look more closely at individual application instances. A high number of users, for example, can lead to performance degradation, and should be investigated.

Figure 26. Summary - Application view

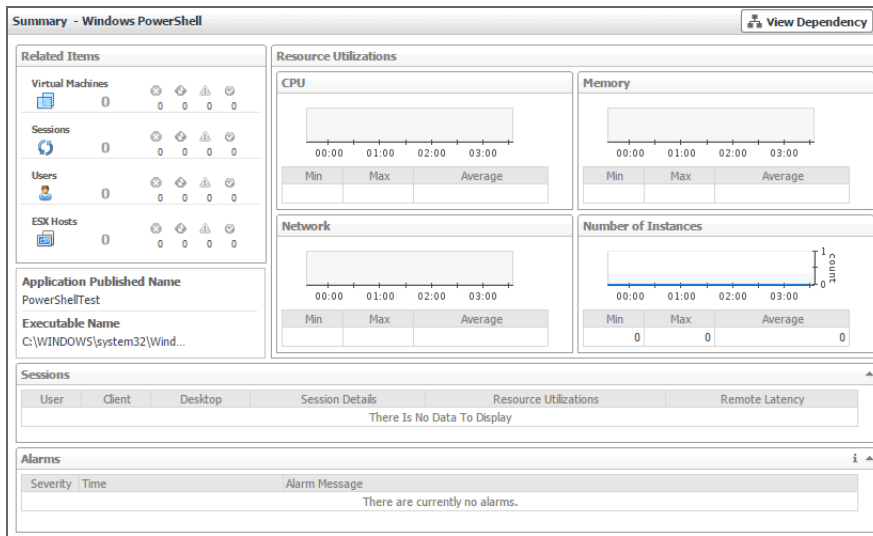
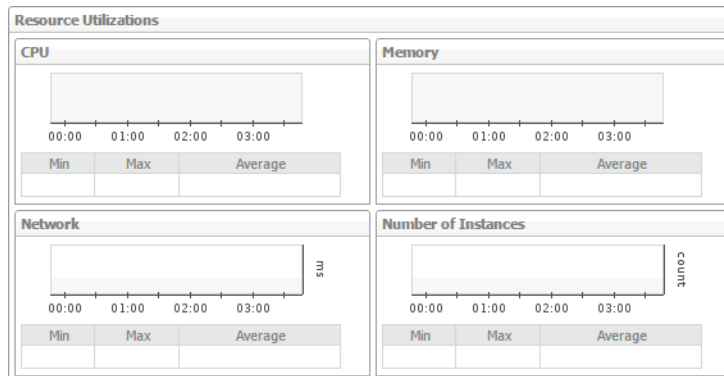


Table 8. Summary - Application view

The minimum, maximum, and average values of CPU and memory utilization, network latency, and application instances, over the selected time range.

Resource Utilizations



The objects that are associated with the selected application and their alarm state.

Related Items

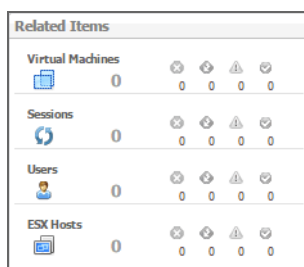


Table 8. Summary - Application view

Application Published Name The name of the application published in your XenDesktop environment and the path to the application executable.

Executable Name	Application Published Name PowerShellTest
	Executable Name C:\WINDOWS\system32\Wind...

General information about the current application sessions, such as the name of the user associated with it, client name, desktop name, additional session details, resource utilization, and latency.

Sessions

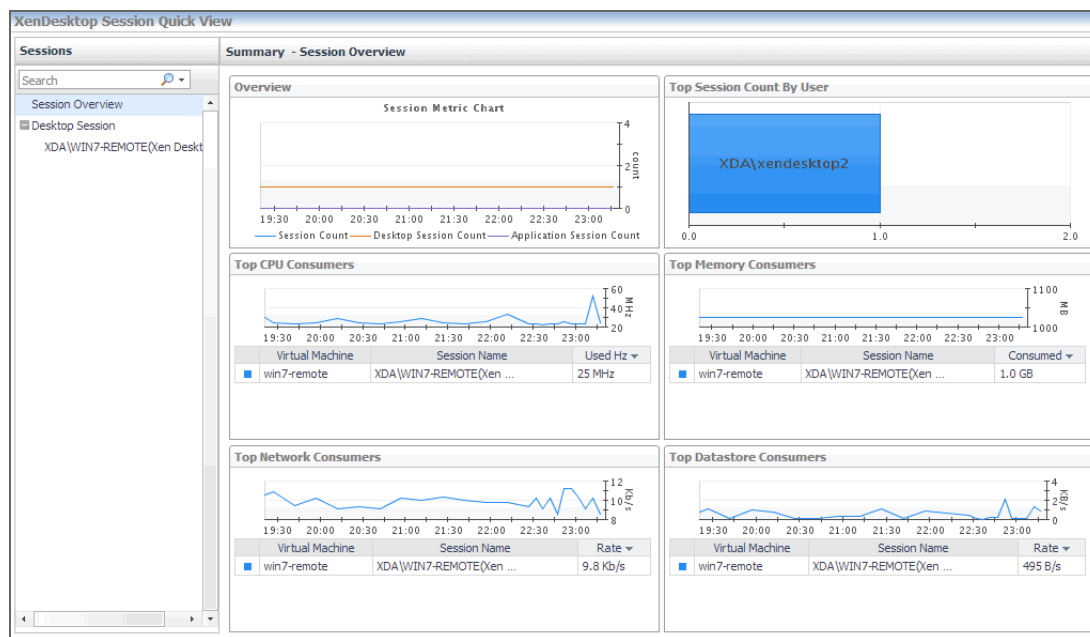
User	Client	Desktop	Session Details	Resource Utilizations	Remote Latency
There Is No Data To Display					

Monitoring Sessions

When an end user obtains access to a virtual desktop, this results in a desktop session. A session is a specific instance of an end user's activity. For those desktops that are monitored by NetScaler agents, you can monitor their sessions. To do that, select the **Sessions** tile on the XenDesktop Environment dashboard. The information appearing in the **XenDesktop Session Quick View** can help you discover potential resource-level issues such as high session counts, and to reallocate resources where they are most needed.

TIP: For more information about XenDesktop Session agents, see [Creating NetScaler Agent instances](#) on page 14.

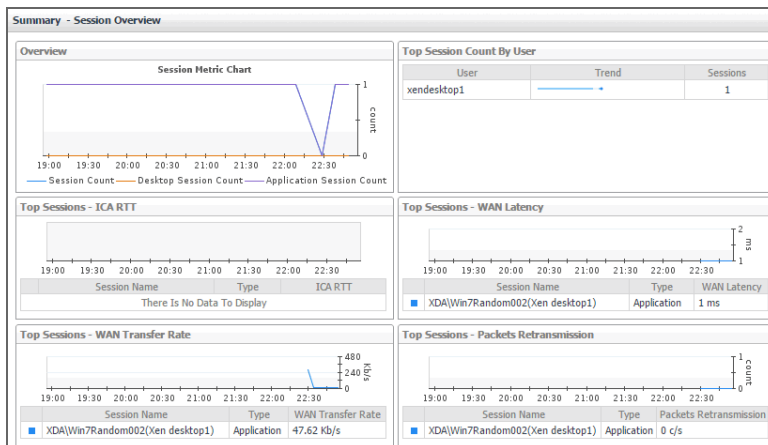
Figure 27. XenDesktop Session Quick View



To explore Sessions:

- 1 On the navigation panel, under **Dashboards**, click **XenDesktop Environment**.
- 2 On the XenDesktop Environment dashboard, on the **Monitoring** tab, click the **Sessions** tile.
- 3 In the **XenDesktop Session Quick View**, in the **Sessions** view on the left, click **Session Overview**.

The **XenDesktop Session Quick View** refreshes, showing the **Summary - Session Overview** view on the right.

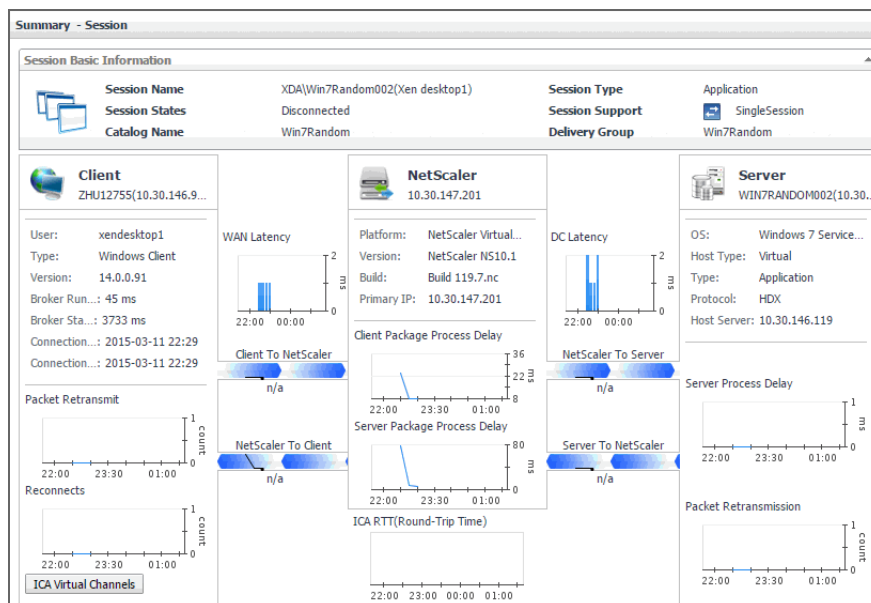


This view identifies the virtual machines that consume the highest amounts of system resources. For more information, see [Observing the Session Overview](#) on page 59.

- 4 In the **Sessions** view, under **Desktop Session** or **Application Session**, click a session.

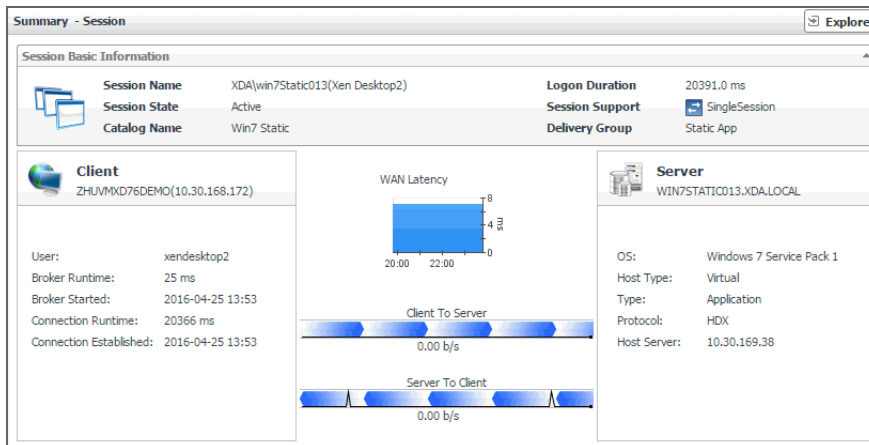
The **XenDesktop Session Quick View** refreshes, showing the **Summary - Session** view on the right.

- If NetScaler data is available, the following information appears on the **Summary - Session** view.



This view displays detailed information about the selected session, such as the session name and type, user logon information, and session performance details. For more information, see [Investigating Session details \(NetScaler data\)](#) on page 61.

- If NetScaler data is not available, the following information appears on the **Summary - Session** view.



This view displays information about the selected session that is collected directly from the host, if you selected the **Collect Session metrics when NetScaler data not available** option in the **XenDesktop Discovery Wizard**. For more information about this view, see [Investigating Session details \(host data\)](#) on page 63. For more information about the **XenDesktop Discovery Wizard**, see [Discovering XenDesktop sites](#) on page 11.

- To find out more about the NetScaler performance, in the **Summary - Session** view, click **NetScaler**. The **NetScaler Performance Detail** dialog box appears.



This dialog box provides in-depth information about the NetScaler performance, such as its CPU and memory utilization, disk space usage, and network transfer rates. For more information, see [NetScaler Performance Details](#) on page 70.

- Explore a session in more detail. In the top-right corner of the view, click **Explore**. The display area refreshes, showing in-depth information about the selected session in the XenDesktop Explorer.



The XenDesktop Explorer can help you to better understand the state of the selected session. Use it to observe the existing resource levels and predict potential bottlenecks that may affect the performance of your monitored system. This intuitive dashboard consists of several tabs, each focusing on a specific aspect of the selected session. For more information, see [Exploring individual Sessions](#) on page 65.

TIP: To return to the XenDesktop Environment dashboard, use the bread crumb trail in the top-left corner.

TIP: You can also explore session details by choosing **XenDesktop > XenDesktop Explorer**, and then selecting a desired session in the **XD Explorer** tree on the navigation panel.

Observing the Session Overview

A session is a specific instance of an end user's activity with a virtual desktop. You can view the performance of desktop or application sessions when you create and configure NetScaler agents to collect ICA (Independent Computing Architecture) session information from monitored Citrix® NetScaler® gateways using Citrix® AppFlow®. For more information about XenDesktop Session agents, see [Creating NetScaler Agent instances](#) on page 14.

To get a good understanding of which desktops or applications consume the highest amounts of system resources, use the **Summary - Session Overview** view. For example, high peaks in the Session Metric Chart can

indicate a sudden increase in the end-users' activity that may result in compromised performance. This view can help you discover potential resource bottlenecks, and to reallocate resources where they are most needed.

Figure 28. Summary - Session Overview

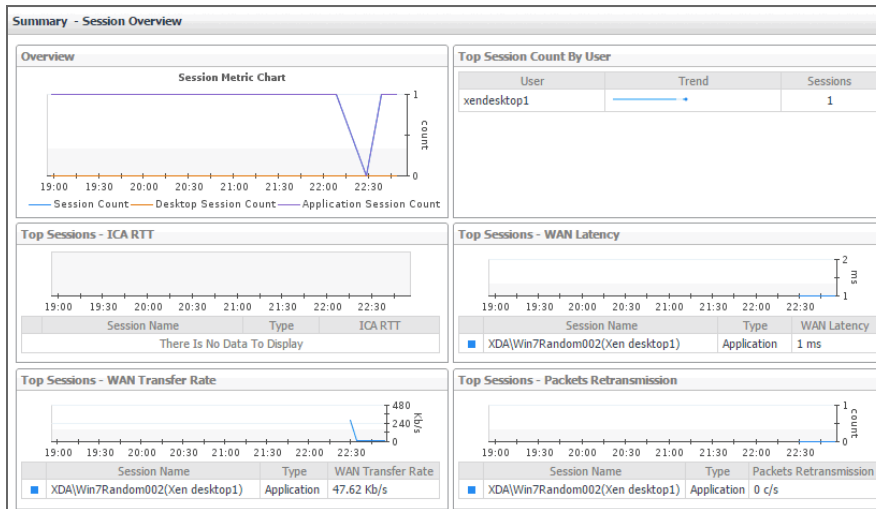
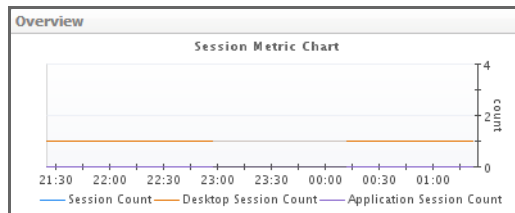


Table 9. Summary - Session Overview

Displays the session counts over the monitored time range. The **Session Count** line in the **Session Metric Chart** shows the number of all sessions. **Desktop Session Count** represents the number of desktop sessions, while **Application Session Count** is the number of application sessions, all during the monitored time range.

Overview



Identifies the users with the highest number of sessions. Each line in the table shows the user name, the trend in the counts of sessions initiated by that end user, and the current number of sessions that user is running.

Top Session Count by User

User	Trend	Sessions
xendesktop1	↔	1

Identifies the ICA sessions with the highest round-trip time (RTT). Each line in the table shows the session name, its type (**Desktop** or **Application**) and its ICA RTT.

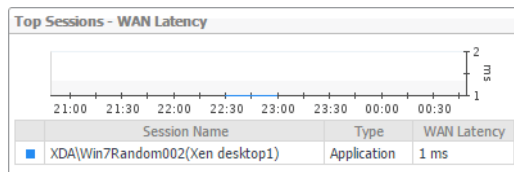
Top Sessions - ICA RTT

Session Name	Type	ICA RTT
There Is No Data To Display		

Table 9. Summary - Session Overview

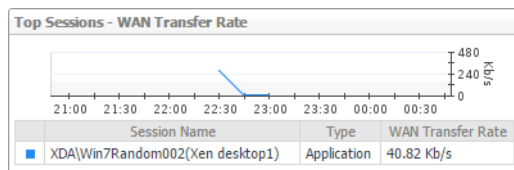
Identifies the sessions with the highest WAN latency. Each line in the table shows the session name, its type (**Desktop** or **Application**) and its WAN latency.

Top Sessions - WAN Latency



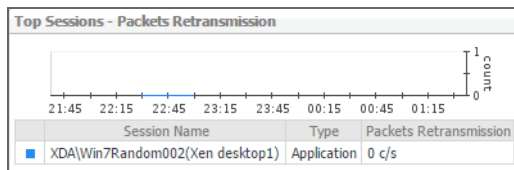
Identifies the sessions with the highest WAN data transfer rates. Each line in the table shows the session name, its type (**Desktop** or **Application**) and the data transfer rate over the WAN.

Top Sessions - WAN Transfer Rate



Identifies the sessions with the highest packet retransmission rates. Data packets are typically re-sent after being lost or damaged. High data retransmission rates are typically caused by network congestion. Each line in the table shows the session name, its type (**Desktop** or **Application**) and the data transfer rate over the WAN.

Top Sessions - Packets Retransmission



Investigating Session details (NetScaler data)

Information about a specific session can give you a good understanding about the end-user's experience with virtual desktops and applications. NetScaler agents collect data about specific sessions, which populates the **Summary - Session** view. Use this view to better understand how end users interact with individual desktops and applications, and to how well your system responds to end-users' requests. For example, high peaks in the latency data may indicate bottlenecks in desktop and application sessions and should be investigated. For more information about NetScaler agents, see [Creating NetScaler Agent instances](#) on page 14.

Figure 29. Summary - Session view (NetScaler data)

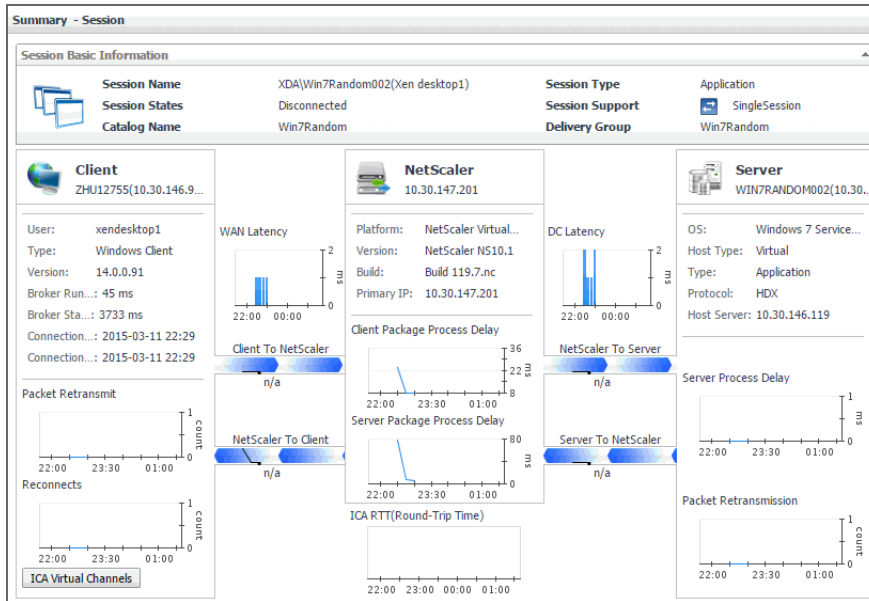
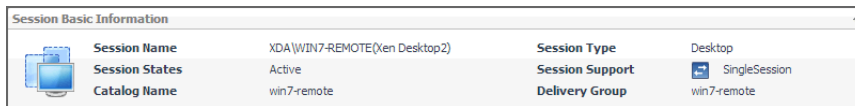


Table 10. Summary - Session view (NetScaler data)

General information about the session, such as its name, state, catalog name, type (desktop or application), support type, and the delivery group to which it belongs.

Session Basic Information



A monitoring dashboard that visualizes the main components in the selected session and their connectivity. This can help you understand the effect of these components may have on your system. Along with displaying the client, NetScaler gateway, and the application or desktop server, this intuitive view connects these elements with a series of graphical flows illustrating the transmission of the session data. For example, you can review the rates of data and flowing between the client, NetScaler gateway, and the application or desktop server, and identify any signs of potential network congestion that may affect your system.

Session Performance Details

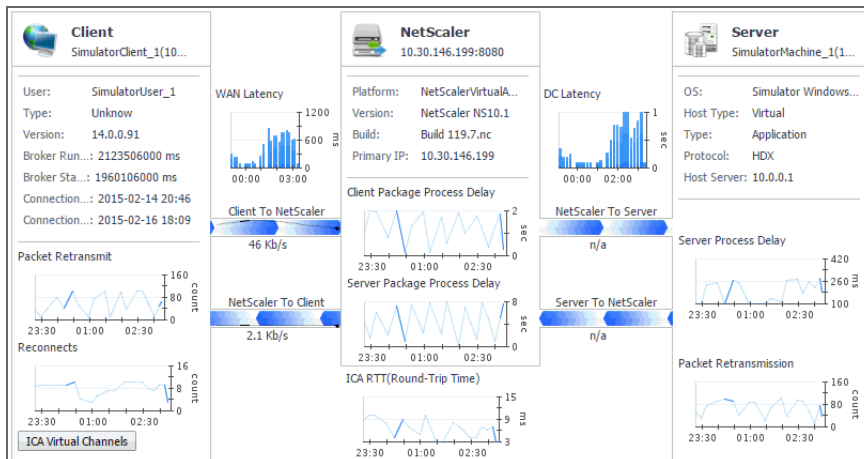


Table 10. Summary - Session view (NetScaler data)

Client: This embedded view shows the name and IP address of the machine accessing your XenDesktop environment. It also displays the following information:

- **User:** The name of the XenDesktop user.
- **Type, Version:** The name and version number of the OS running on the client machine.
- **Broker Runtime:** The amount of time the connection broker process has been running during its most recent connection attempt.
- **Broker Started:** The amount of time that has passed since the broker process for the first time.
- **Connection Runtime:** The date and time when the connection broker process has connected during its most recent connection attempt.
- **Connection Established:** The date and time when the connection broker process has established the connection for the first time.
- **Packet Retransmit:** The number of times data packets are re-sent after being lost or damaged over the selected time range.
- **Reconnects:** The number of times the connection had to be re-established over the selected time range.
- **WAN Latency:** The WAN latency rates between the client and the NetScaler gateway, over the selected time range.

NetScaler: This embedded view shows the name and IP address of the NetScaler gateway machine. It also displays the following information:

- **Platform:** The name of the NetScaler appliance.
- **Version, Build:** The NetScaler version and build numbers.
- **Primary IP:** The IP address of the NetScaler appliance.
- **Client Package Process Delay:** The amount of time the client package is delayed, over the selected time range.
- **Server Package Process Delay:** The amount of time the server package is delayed, over the selected time range.
- **ICA RTT (Round-Trip Time):** The length of the ICA RTT over the selected time range.
- **DC Latency:** The data center (DC) latency rates between the NetScaler gateway and the application or desktop server, over the selected time range.

Server: This embedded view shows the name and IP address of the XenDesktop server machine hosting the application or desktop associated with the selected session. It also displays the following information:

- **OS:** The name and version of the OS running on the server.
- **Host Type:** The type of the host (**Physical** or **Virtual**) on which the XenDesktop server is running.
- **Type:** The session type (**Application** or **Desktop**).
- **Protocol:** The remote display protocol (for example, **HDX**).
- **Host Server:** The IP address of the host machine on which the server is running.
- **Server Process Delay:** The amount of time the server process is delayed, over the selected time range.
- **Packet Retransmission:** The number of times data packets are re-sent after being lost or damaged, over the selected time range.

Investigating Session details (host data)

Information about a specific session can give you a good understanding about the end-user's experience with virtual desktops and applications. These metrics are typically collected by NetScaler agents. However, if NetScaler data is not available, you can collect session metrics directly from the host, if you selected the **Collect Session**

metrics when NetScaler data not available option in the **XenDesktop Discovery Wizard**. For more information about the **XenDesktop Discovery Wizard**, see [Discovering XenDesktop sites](#) on page 11.

When you collect session metrics directly from the host, the **Summary - Session** view can help you understand how well the monitored system responds to client requests in a selected session. It also provides some basic session information, such as the session name, state, catalog name, logon duration, support type, and the delivery group to which it belongs.

Figure 30. Summary - Session view (host data)

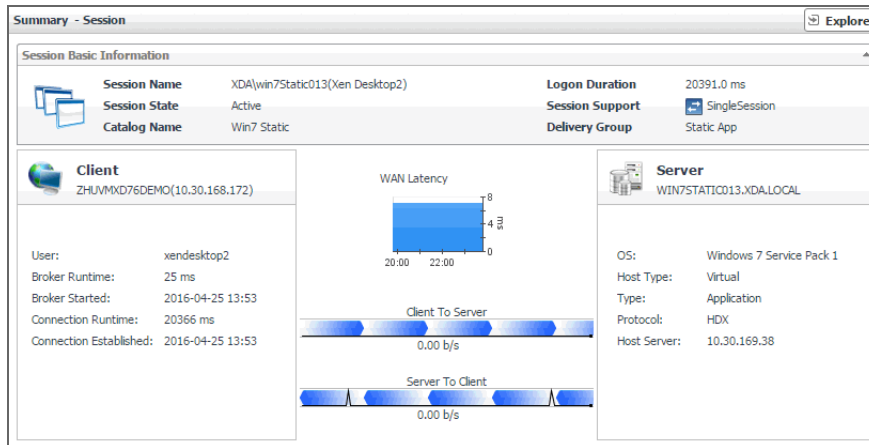



Table 11. Summary - Session view (host data)

General information about the session, such as its name, state, catalog name, logon duration, support type, and the delivery group to which it belongs.

Session Basic Information

Session Basic Information			
	Session Name	XDA\win7Static013(Xen Desktop2)	Logon Duration
	Session State	Active	20391.0 ms
	Catalog Name	Win7 Static	Session Support
			SingleSession
			Delivery Group
			Static App

A monitoring dashboard that visualizes the main components in the selected session and their connectivity. This can help you understand the effect of these components may have on your system. Along with displaying the client, WAN latency metrics, and the application or desktop server, this intuitive view connects these elements with a series of graphical flows illustrating the transmission of the session data. For example, you can review the rates of data and flowing between the client, and the application or desktop server, and identify any signs of potential network congestion that may affect your system.

Session Performance Details

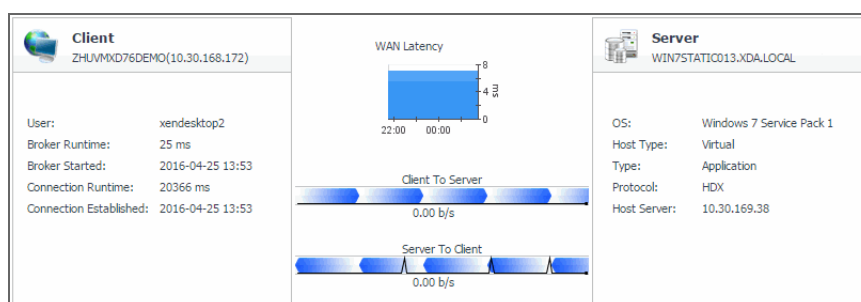


Table 11. Summary - Session view (host data)

Client: This embedded view shows the name and IP address of the machine accessing your XenDesktop environment. It also displays the following information:

- **User:** The name of the XenDesktop user.
- **Broker Runtime:** The amount of time the connection broker process has been running during its most recent connection attempt.
- **Broker Started:** The amount of time that has passed since the broker process for the first time.
- **Connection Runtime:** The date and time when the connection broker process has connected during its most recent connection attempt.
- **Connection Established:** The date and time when the connection broker process has established the connection for the first time.

WAN Latency: This embedded view shows the WAN latency rates over the selected time period and the data transfer rates between the client and the server in each direction, for the selected session.

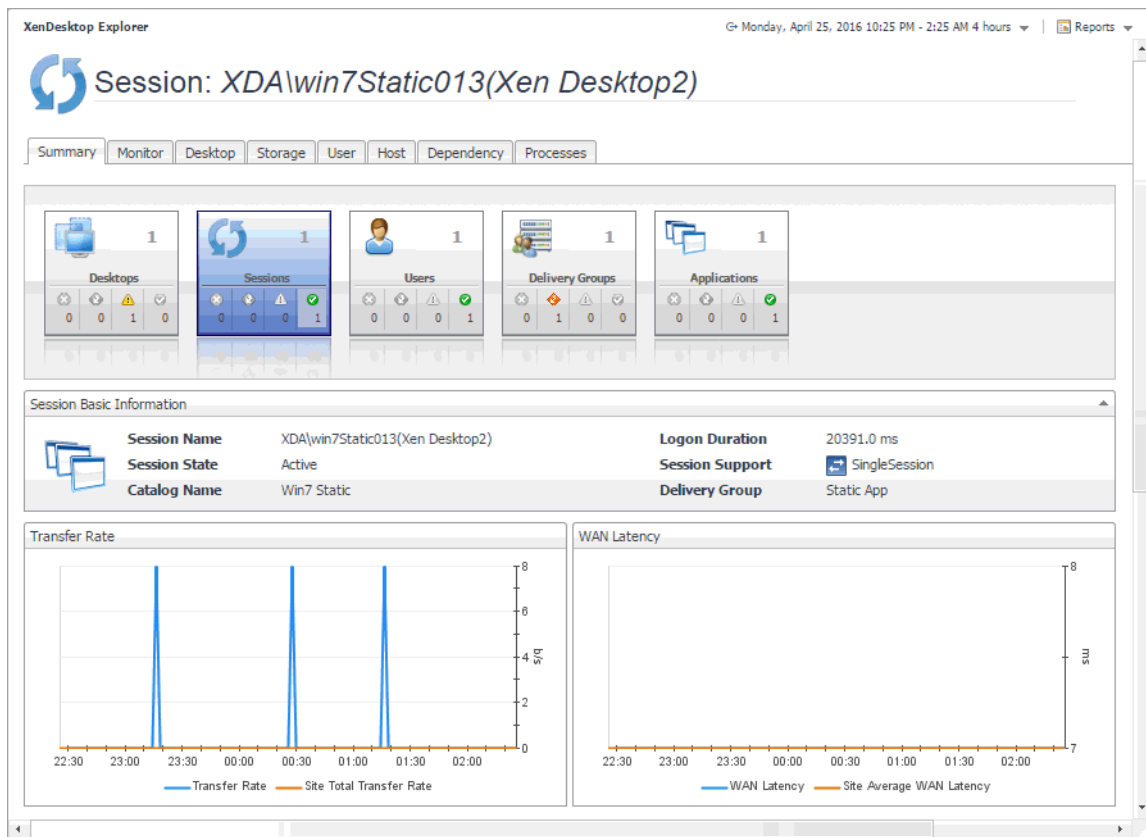
Server: This embedded view shows the name and IP address of the XenDesktop server machine hosting the application or desktop associated with the selected session. It also displays the following information:

- **OS:** The name and version of the OS running on the server.
- **Host Type:** The type of the host (**Physical** or **Virtual**) on which the XenDesktop server is running.
- **Type:** The session type (**Application** or **Desktop**).
- **Protocol:** The remote display protocol (for example, **HDX**).
- **Host Server:** The IP address of the host machine on which the server is running.

Exploring individual Sessions

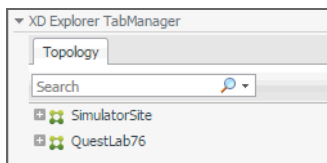
If you see any indicators that could lead to session-related issues, you can explore it in more detail. The XenDesktop Explorer can help you to better understand the state of the selected session. Use it to observe the existing resource levels and predict potential bottlenecks that may affect the performance of your monitored system. This intuitive dashboard consists of several tabs, each focusing on a specific aspect of the selected session.

Figure 31. XenDesktop Explorer: Summary tab

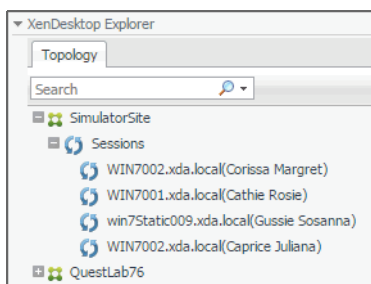


To access the XenDesktop Explorer:

- 1 On the navigation panel, under **Dashboards**, choose **XenDesktop > XenDesktop Explorer**.
The **XD Explorer** view appears on the navigation panel.



- 2 In the **XD Explorer** view, expand the navigation tree to find the session that you want to explore.



The display area refreshes, showing the XenDesktop Explorer dashboard.

i | TIP: Alternatively, you can navigate to this dashboard by selecting a desktop or application session on the XenDesktop Environment dashboard and clicking **Explore**.

For more information about this dashboard, see the following sections:

- [Summary tab](#) on page 67
- [Monitor tab \(NetScaler data\)](#) on page 68
- [Monitor tab \(host data\)](#) on page 73
- [Desktop tab](#) on page 75
- [Storage tab](#) on page 77
- [User tab](#) on page 79
- [Host tab](#) on page 81
- [Dependency tab](#) on page 84
- [Processes tab](#) on page 84

Summary tab

The **Summary** tab is the first tab that appears open by default when you access the XenDesktop Explorer for the first time. It displays general information about the selected session, such as its name, state, catalog name, type (desktop or application), support type, and the delivery group to which it belongs. This tab also provides a set of graphs that illustrate the rates of the selected session's round-trip time, WAN latency, WAN data transfer rates, and packet retransmission rates over the selected time range. Use that information to better understand how the session performs during a selected time period. Average site rates are also displayed, for comparison. In general, consistently high peaks in the graphs may indicate the signs of potential bottlenecks and should be investigated.

Figure 32. XenDesktop Explorer: Summary tab

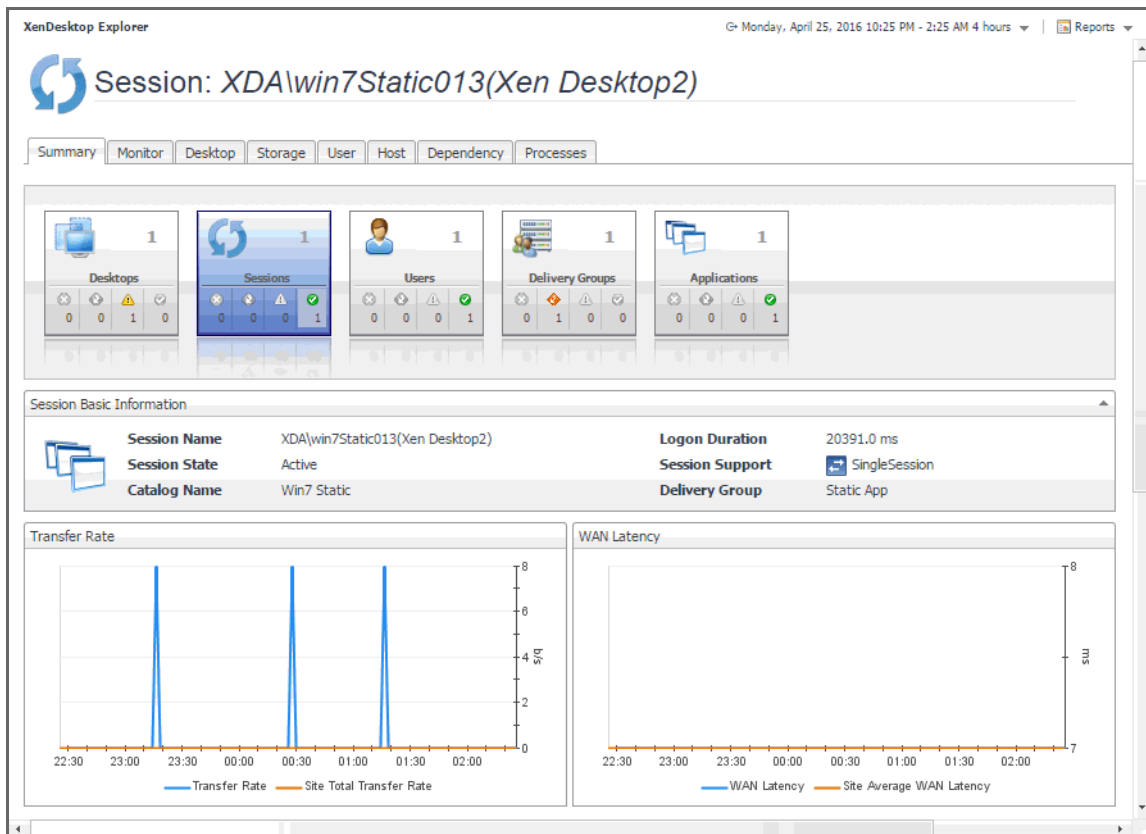




Table 12. XenDesktop Explorer: Summary tab

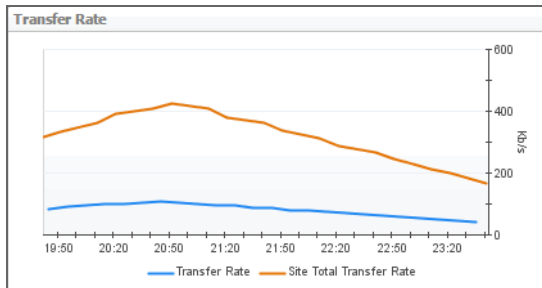
General information about the session, such as its name, state, catalog name, type (desktop or application), support type, and the delivery group to which it belongs.

Session Basic Information

Session Basic Information				
	Session Name	XDA WIN7-REMOTE(Xen Desktop2)	Session Type	Desktop
	Session States	Active	Session Support	 SingleSession
	Catalog Name	win7-remote	Delivery Group	win7-remote

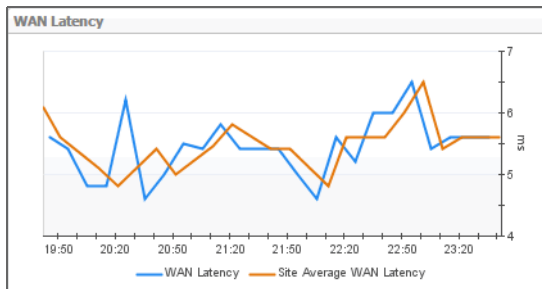
Displays the session's WAN data transfer rates over the selected tile range. It also shows the average WAN data transfer rates for all sessions that belong to the same XenDesktop site.

Transfer Rate



Displays the session's WAN latency over the selected tile range. It also shows the average WAN latency rates for all sessions that belong to the same XenDesktop site.

WAN Latency



Monitor tab (NetScaler data)

The **Monitor tab** visualizes the main components in the selected session and their connectivity. This can help you understand the effect of these components may have on your system. Along with displaying the client, NetScaler gateway, and the application or desktop server, this intuitive dashboard connects these elements with a series of graphical flows illustrating the transmission of the session data. For example, you can review the rates of data and flowing between the client, NetScaler gateway, and the application or desktop server, and identify any signs of potential network congestion that may affect your system.

Figure 33. XenDesktop Explorer: Monitor tab (NetScaler data)

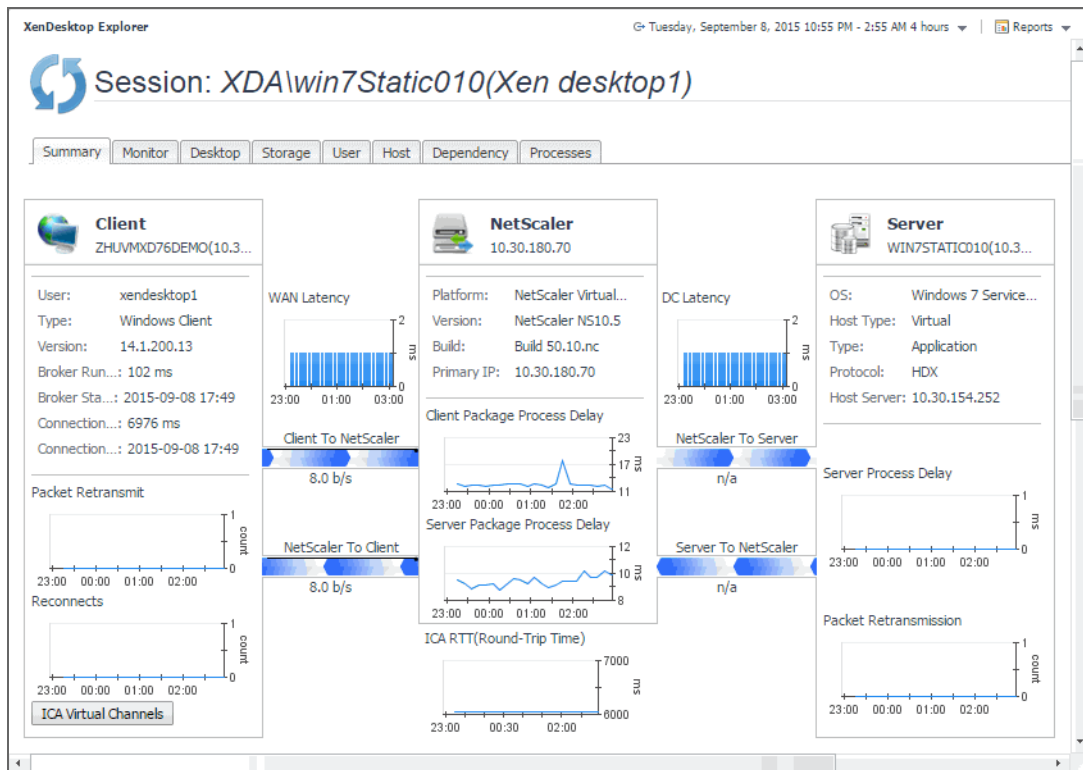


Table 13. XenDesktop Explorer: Monitor tab (NetScaler data)

	<p>This embedded view shows the name and IP address of the machine accessing your XenDesktop environment. It also displays the following information:</p> <ul style="list-style-type: none">• User: The name of the XenDesktop user.• Type, Version: The name and version number of the OS running on the client machine.• Broker Runtime: The amount of time the connection broker process has been running during its most recent connection attempt.• Broker Started: The amount of time that has passed since the broker process for the first time.
Client	<ul style="list-style-type: none">• Connection Runtime: The date and time when the connection broker process has connected during its most recent connection attempt.• Connection Established: The date and time when the connection broker process has established the connection for the first time.• Packet Retransmit: The number of times data packets are re-sent after being lost or damaged over the selected time range.• Reconnects: The number of times the connection had to be re-established over the selected time range.• WAN Latency: The WAN latency rates between the client and the NetScaler gateway, over the selected time range. <p>This embedded view shows the name and IP address of the NetScaler gateway machine. It also displays the following information:</p> <ul style="list-style-type: none">• Platform: The name of the NetScaler appliance.• Version, Build: The NetScaler version and build numbers.• Primary IP: The IP address of the NetScaler appliance.• Client Package Process Delay: The amount of time the client package is delayed, over the selected time range.• Server Package Process Delay: The amount of time the server package is delayed, over the selected time range.• ICA RTT (Round-Trip Time): The length of the ICA RTT over the selected time range.• DC Latency: The data center (DC) latency rates between the NetScaler gateway and the application or desktop server, over the selected time range. <p>This embedded view shows the name and IP address of the XenDesktop server machine hosting the application or desktop associated with the selected session. It also displays the following information:</p> <ul style="list-style-type: none">• OS: The name and version of the OS running on the server.• Host Type: The type of the host (Physical or Virtual) on which the XenDesktop server is running.
NetScaler	
Server	<ul style="list-style-type: none">• Type: The session type (Application or Desktop).• Protocol: The remote display protocol (for example, HDX).• Host Server: The IP address of the host machine on which the server is running.• Server Process Delay: The amount of time the server process is delayed, over the selected time range.• Packet Retransmission: The number of times data packets are re-sent after being lost or damaged, over the selected time range.

NetScaler Performance Details

The **NetScaler Performance Detail** dialog box provides in-depth information about the NetScaler performance, such as its CPU and memory utilization, disk space usage, and network transfer rates. To display this dialog box, click **NetScaler** in the **XenDesktop Session Quick View** (see [Investigating Session details \(NetScaler data\)](#)) or on the **Monitor** tab of the XenDesktop Explorer (see [Monitor tab \(NetScaler data\)](#)).

Figure 34. NetScaler Performance Detail

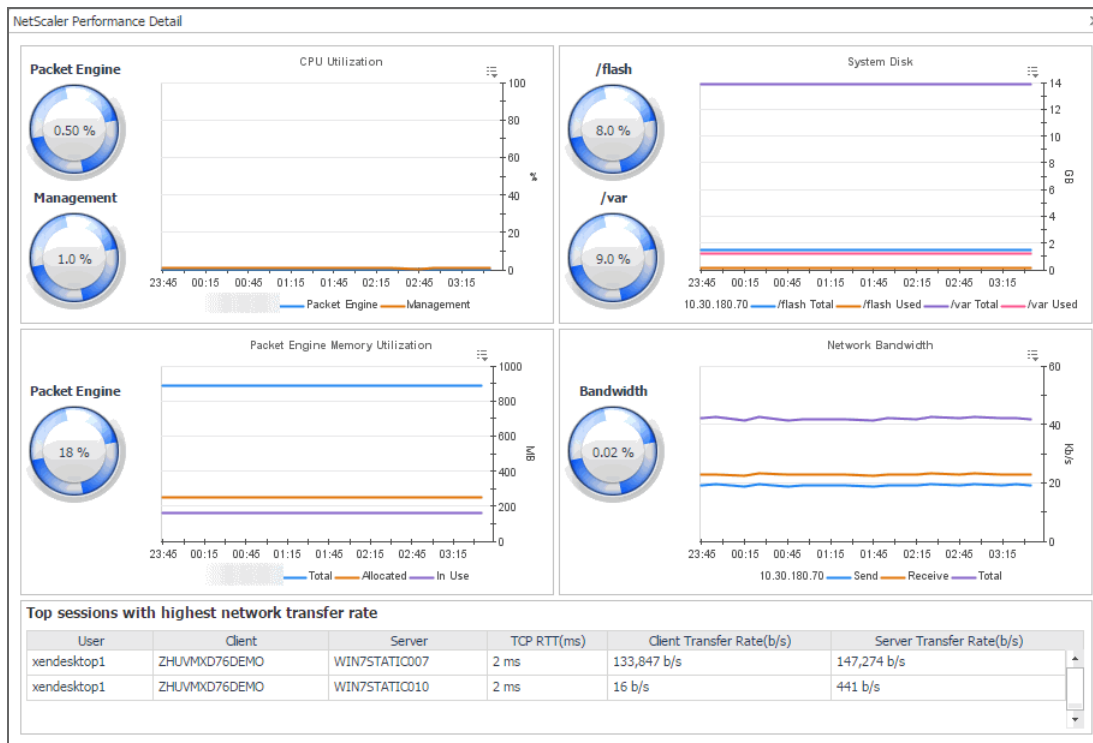
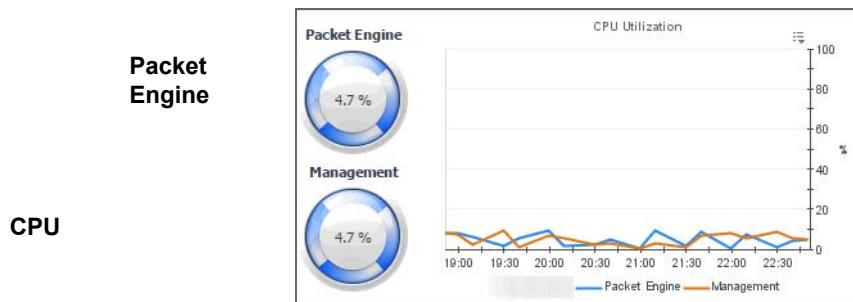


Table 14. Summary - Desktop view

The **Packet Engine** spinner indicates the current percentage of the NetScaler CPU load, used to process data packets, based on the total CPU capacity. The NetScaler packet engine collects data packets from the network and processes them. An efficient packet engine can process data packets in microseconds, optimizing application delivery and overall user experience.

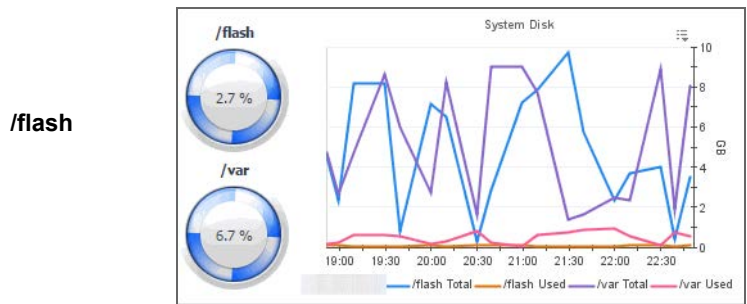


The **Management** spinner indicates the current percentage of the NetScaler CPU load, used to process management functions, based on the total CPU capacity. Management functions include activities such as SNMP communications and management console access. Reserving capacity for management features allows the administrator to efficiently manage the system during heavy traffic loads.

The **Packet Engine** line in the **CPU Utilization** chart shows the percentage of the NetScaler CPU load used to process data packets, during the selected time period. The **Management** line in the chart shows the percentage of the NetScaler CPU load used to process management functions, during the selected time period.

Table 14. Summary - Desktop view

The **/flash** spinner indicates the current percentage of the total storage space used by the mounted flash device.



/flash

Disk

/var

The **/var** spinner indicates the current percentage of the total storage space used by the NetScaler hard drive.

The **/flash Total** line in the **System Disk** chart shows the total amount of space available on the flash device, during the selected time period.

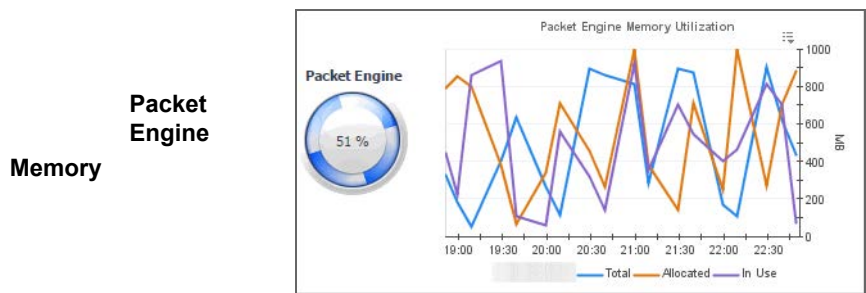
The **/flash Used** line in the chart represents the total amount of the flash device space used during the selected time period.

System Disk

The **/var Total** line shows the total amount of the available hard disk space, during the selected time period.

The **/var Used** line in the chart represents the total amount of the hard disk space used during the selected time period.

The **Packet Engine** spinner indicates the current percentage of the NetScaler memory load used to process data packets, based on the total memory capacity.



Packet Engine

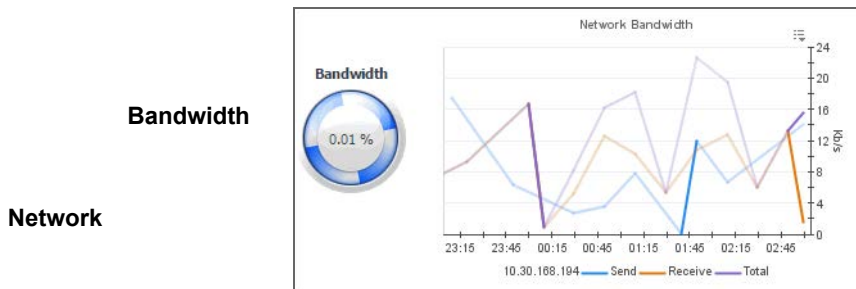
Memory

Packet Engine

The **Utilization** line in the **Memory Utilization** chart shows the percentage of memory used by the virtual machine during the selected time period. The **Baseline** area in the chart indicates the expected memory utilization range based on historical data.

Table 14. Summary - Desktop view

The **Bandwidth** spinner indicates the current percentage of the NetScaler network bandwidth that is currently in use, based on the total memory capacity.



Bandwidth

Network

Network Bandwidth

The **Send** line in the **Network Bandwidth** chart shows the rate at which NetScaler sends data to the network during the selected time period.

The **Receive** line in the **Network Bandwidth** chart shows the rate at which NetScaler receives data from the network during the selected time period.

The **Total** line in the **Network Bandwidth** chart shows the rate at which NetScaler receives and sends data to the network during the selected time period.

Top sessions with highest network rate

This table identifies the sessions with the highest data transfer rates. For each session, it identifies the user, desktop, and delivery controller associated with the session. It also displays delivery controller and desktop data transfer rates, and the TCP round-trip times.

Top sessions with highest network transfer rate						
User	Client	Server	TCP RTT(ms)	Client Transfer Rate(b/s)	Server Transfer Rate(b/s)	
xendesktop1	ZHUVMXD76DEMO	WIN7STATIC007	2 ms	133,847 b/s	147,274 b/s	
xendesktop1	ZHUVMXD76DEMO	WIN7STATIC010	2 ms	16 b/s	441 b/s	

Monitor tab (host data)

The **Monitor tab** visualizes the main components in the selected session and their connectivity. This can help you understand the effect of these components may have on your system. These metrics are typically collected by NetScaler agents. However, if NetScaler data is not available, you can collect session metrics directly from the host, if you selected the **Collect Session metrics when NetScaler data not available** option in the **XenDesktop Discovery Wizard**. For more information about the **XenDesktop Discovery Wizard**, see [Discovering XenDesktop sites](#) on page 11.

When you collect session metrics directly from the host, the **Monitor** tab can help you understand how well the monitored system responds to client requests in a selected session. It also provides some basic session information, such as the session name, state, catalog name, logon duration, support type, and the delivery group to which it belongs.

Figure 35. XenDesktop Explorer: Monitor tab (host data)

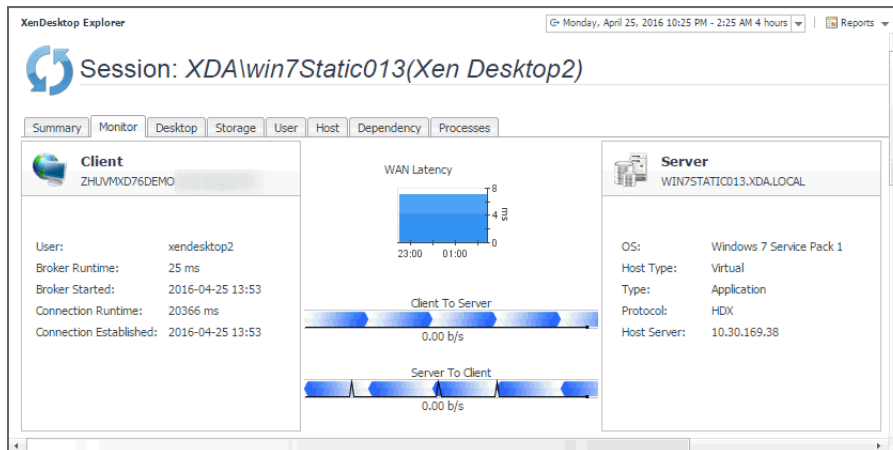


Table 15. XenDesktop Explorer: Monitor tab (host data)

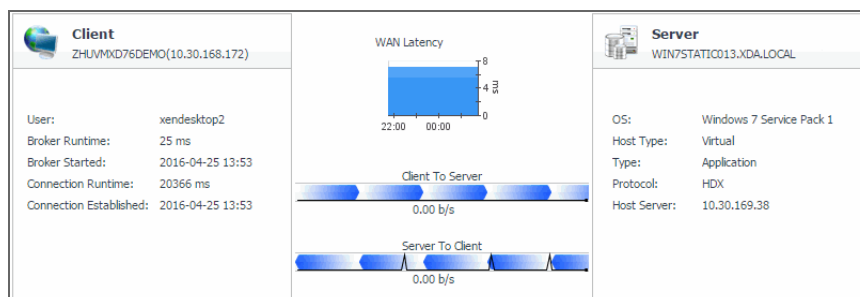
General information about the session, such as its name, state, catalog name, logon duration, support type, and the delivery group to which it belongs.

Session Basic Information

Session Basic Information				
	Session Name	XDA\win7Static013(Xen Desktop2)	Logon Duration	20391.0 ms
	Session State	Active	Session Support	SingleSession
	Catalog Name	Win7 Static	Delivery Group	Static App

A monitoring dashboard that visualizes the main components in the selected session and their connectivity. This can help you understand the effect of these components may have on your system. Along with displaying the client, WAN latency metrics, and the application or desktop server, this intuitive view connects these elements with a series of graphical flows illustrating the transmission of the session data. For example, you can review the rates of data and flowing between the client, and the application or desktop server, and identify any signs of potential network congestion that may affect your system.

Session Performance Details



Client: This embedded view shows the name and IP address of the machine accessing your XenDesktop environment. It also displays the following information:

- **User:** The name of the XenDesktop user.
- **Broker Runtime:** The amount of time the connection broker process has been running during its most recent connection attempt.
- **Broker Started:** The amount of time that has passed since the broker process for the first time.
- **Connection Runtime:** The date and time when the connection broker process has connected during its most recent connection attempt.
- **Connection Established:** The date and time when the connection broker process has established the connection for the first time.

Table 15. XenDesktop Explorer: Monitor tab (host data)

WAN Latency: This embedded view shows the WAN latency rates over the selected time period and the data transfer rates between the client and the server in each direction, for the selected session.

Server: This embedded view shows the name and IP address of the XenDesktop server machine hosting the application or desktop associated with the selected session. It also displays the following information:

- **OS:** The name and version of the OS running on the server.
- **Host Type:** The type of the host (**Physical** or **Virtual**) on which the XenDesktop server is running.
- **Type:** The session type (**Application** or **Desktop**).
- **Protocol:** The remote display protocol (for example, **HDX**).
- **Host Server:** The IP address of the host machine on which the server is running.

Desktop tab

In your monitored environment, a Desktop component encapsulates a Windows® desktop together with application elements that are delivered to end-users on demand. You can review the performance of individual desktops on the **Desktop** tab. This tab shows the usage of system resources for the desktop associated with the selected session. Use it to see the trends in usage of the selected component's system resources, and to review any generated alarms, if they exist. For example, high peaks in the memory utilization chart, that drastically exceed historical values could result in performance degradation and should be investigated.

Figure 36. XenDesktop Explorer: Desktop tab

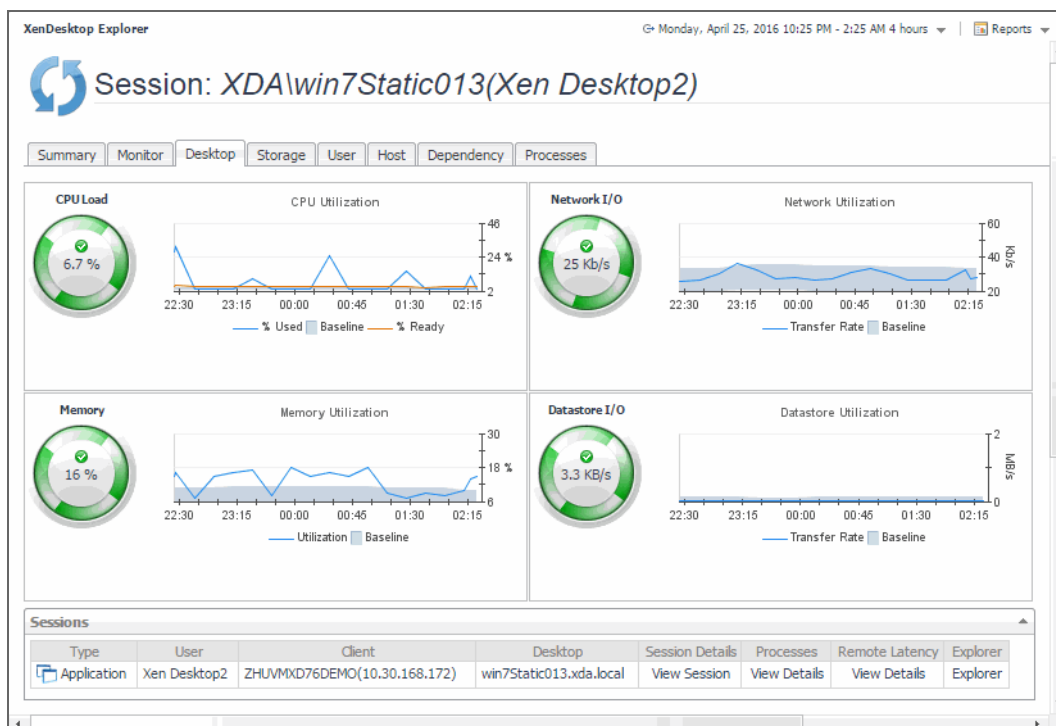


Table 16. XenDesktop Explorer: Desktop tab

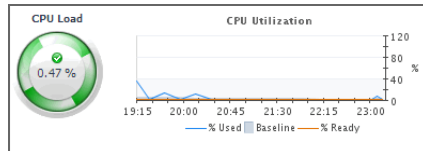
The **CPU Load** spinner indicates the current percentage of the selected virtual machine's CPU load, used to execute system code and user programs, based on the total CPU capacity.

The **% Used** line in the **CPU Utilization** chart shows the percentage of the CPU utilization used by the virtual machine to execute system code and user programs, during the selected time period.

% Ready displays the percentage of the virtual machine's CPU resources that are ready to execute system code and user programs during the selected time period.

CPU

The **Baseline** area in the chart indicates the expected CPU utilization range based on historical data.

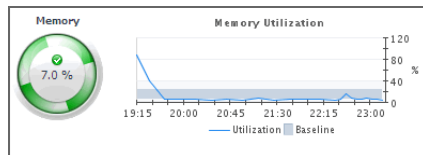


The **Memory** spinner indicates the current percentage of the average memory usage by the selected virtual machine, based on the total memory capacity.

The **Utilization** line in the **Memory Utilization** chart shows the percentage of memory used by the virtual machine during the selected time period.

The **Baseline** area in the chart indicates the expected memory utilization range based on historical data.

Memory



The **Datastore I/O** spinner indicating the current datastore I/O rate the selected virtual machine utilizes, based on the total datastore capacity.

The **Transfer Rate** line in the **Datastore Utilization** chart shows the rate at which the virtual machine reads and writes data to the datastore during the selected time period.

The **Baseline** area in the chart indicates the expected datastore utilization range based on historical data.

Datastore I/O

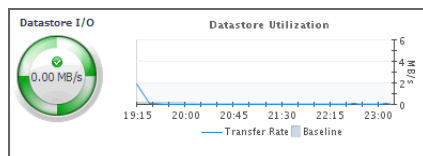


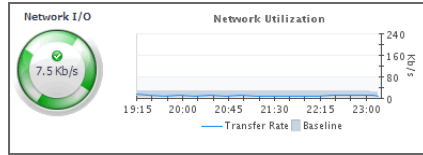
Table 16. XenDesktop Explorer: Desktop tab

The **Network I/O** spinner indicates the current rate at which the selected virtual machine transfers data from and to the network.

The **Transfer Rate** line in the **Network Utilization** chart shows the rate at which the selected virtual machine receives and sends data to the network during the selected time period.

The **Baseline** area in the chart indicates the expected network utilization range based on historical data.

Network I/O



General information about the session, such as its type (desktop or application), the user running the session, client name, desktop name, additional session details, resource utilization, and latency.

Sessions

Type	User	Client	Desktop	Session Details	Resource Utilization	Remote Latency	Explorer
Desktop	Caprice Juliana	Caprice_Juliana(10.0.0.9)	WIN7002.xda.local	View Session	View Details	View Details	Explorer

Storage tab

The **Storage** tab displays a combination of embedded views illustrating the storage capacity available to the datastores associated with the selected session. It identifies the datastores associated with the selected virtual machine and shows performance metrics associated with each datastore.

Figure 37. XenDesktop Explorer: Storage tab

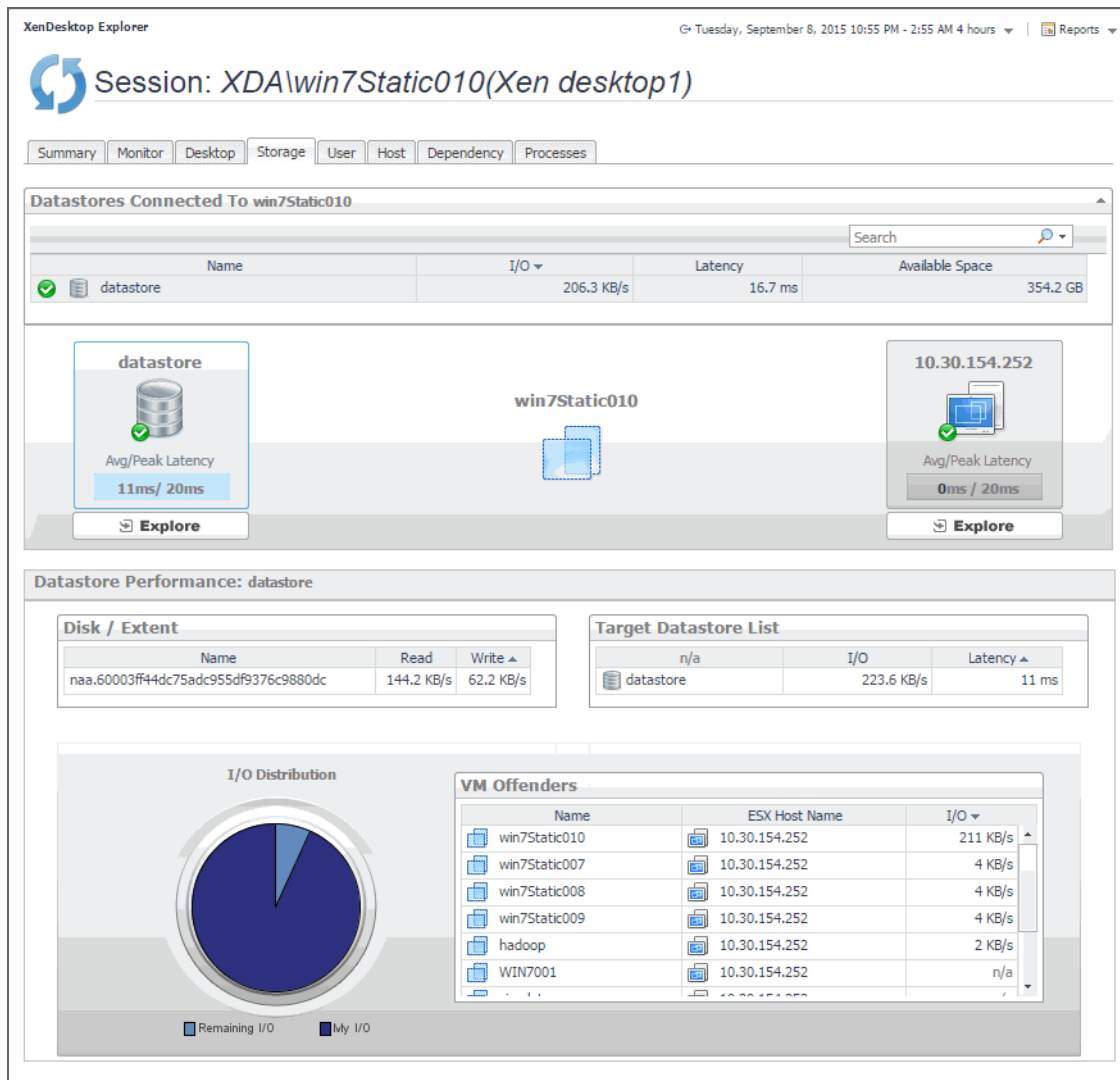


Table 17. XenDesktop Explorer: Storage tab

Datastores Connected To	Name	The datastore name and its alarm status.
	I/O	The datastore data transfer rates associated with the physical host.
	Latency	The datastore latency.
	Available Space	The amount of available space on the datastore.
	Datastore, Avg/Peak Latency	The average and peak latency rates for the selected datastore.
Datastore Performance	Physical host, Avg/Peak Latency	The average and peak latency rates for the physical host.
	Name	The name of the disk associated with the datastore.
	Disk/Extent	
	Read	The read rate of the disk associated with the datastore.
	Write	The write rate of the disk associated with the datastore.

Table 17. XenDesktop Explorer: Storage tab

Target Name	The name of the target datastore.
Datastore I/O	The data transfer rate of the target datastore.
List Latency	The data transfer latency of the target datastore.
I/O Distribution	A pie chart indicating how much the selected virtual machines contributes to the overall use of I/O resources.
VM Offenders Name	The name of the virtual desktop.
ESX	The name of the ESX host on which the virtual desktop is running.
Host Name	
I/O	The data transfer rate for the virtual desktop.

User tab

The **User** tab displays set of graphs that illustrate the rates of the selected session's data packet retransmission and transfer rates on the client and server side. In general, consistently high values in the graphs may indicate the signs of potential bottlenecks and should be investigated.

Figure 38. XenDesktop Explorer: User tab

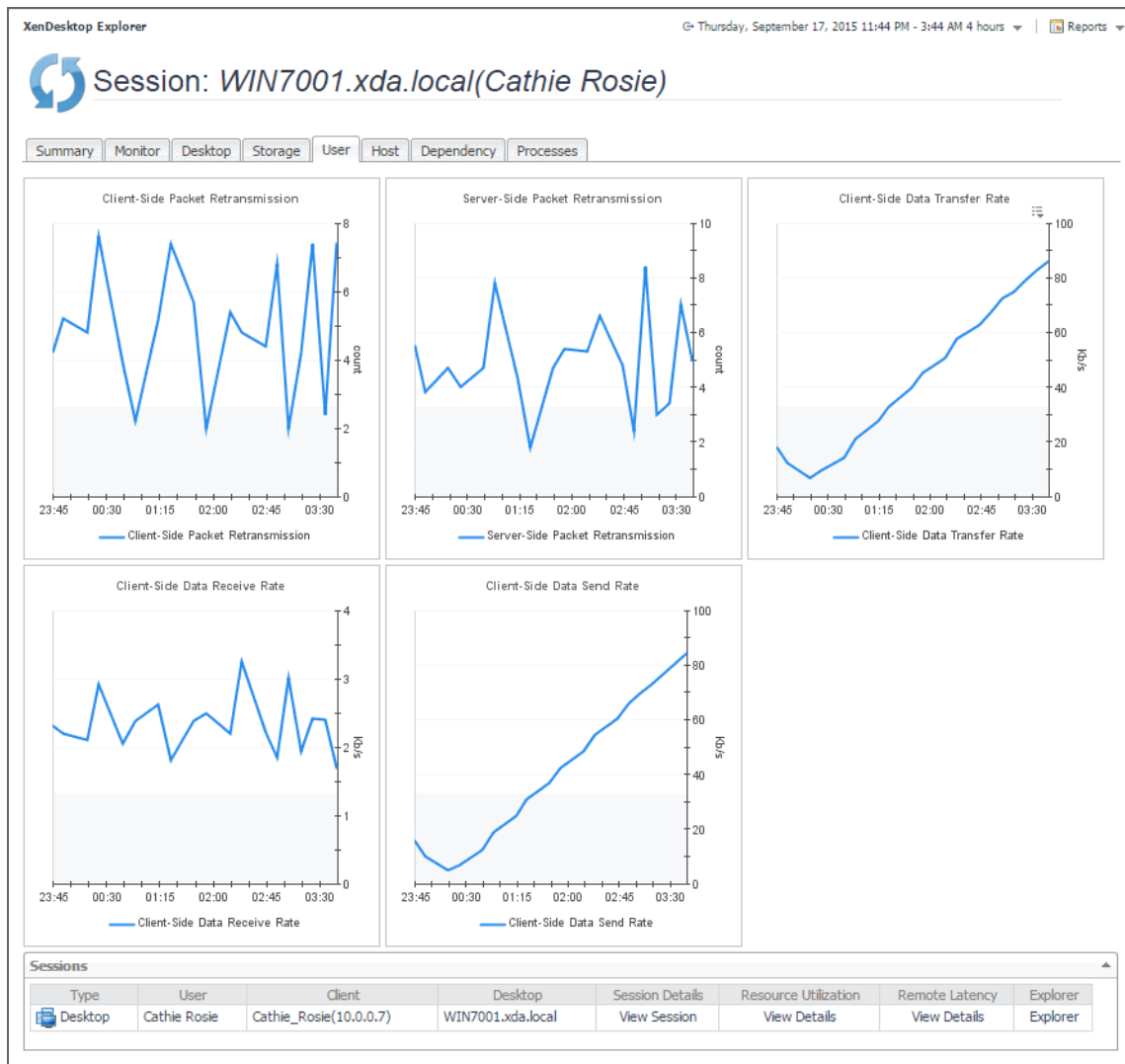
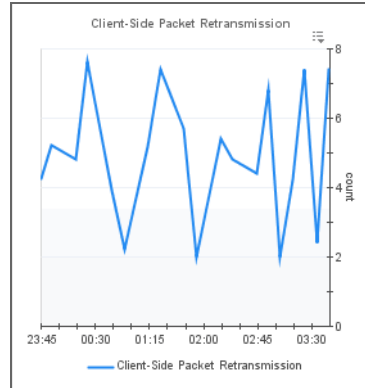


Table 18. XenDesktop Explorer: User tab

The number of times data packets are re-sent from the virtual desktop client after being lost or damaged over the selected time range. High data retransmission rates are typically caused by network congestion.

Figure 39. Client-Side Packet Retransmission view

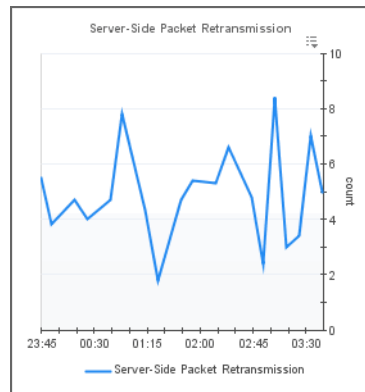
Client-Side Packet Retransmission



The number of times data packets are re-sent from the XenDesktop site after being lost or damaged over the selected time range.

Figure 40. Server-Side Packet Retransmission view

Server-Side Packet Retransmission



The rate at which the virtual desktop client receives and sends data packets over the selected time range.

Figure 41. Client-Side Data Transfer Rate view

Client-Side Data Transfer Rate

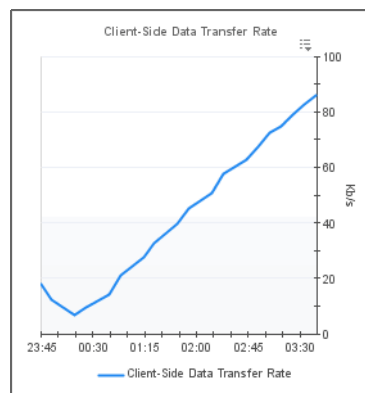
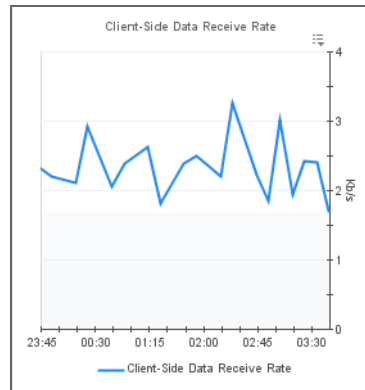


Table 18. XenDesktop Explorer: User tab

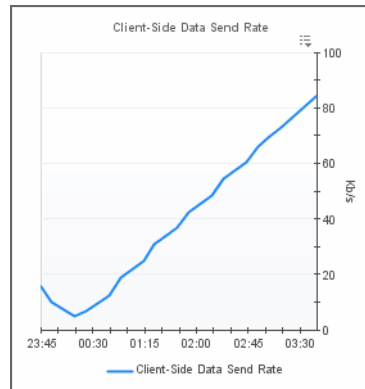
The rate at which the virtual desktop client receives data packets over the selected time range.

Client-Side Data Receive Rate



The rate at which the virtual desktop client sends data packets over the selected time range.

Client-Side Data Send Rate



General information about the session, such as its type (desktop or application), the user running the session, client name, desktop name, additional session details, resource utilization, and latency.

Sessions

Type	User	Client	Desktop	Session Details	Resource Utilization	Remote Latency	Explorer
Desktop	Caprice Juliana	Caprice_Juliana(10.0.0.9)	WIN7002.xda.local	View Session	View Details	View Details	Explorer

Host tab

The **Host** tab shows the usage of system resources for the physical host associated with the selected session. Use it to see the trends in usage of the host's system resources, to see which virtual desktops and sessions are running on the host, and to look for the signs of compromised performance. For example, high peaks in the memory utilization chart, that drastically exceed historical values could result in performance degradation and should be investigated.

Figure 42. XenDesktop Explorer: Host tab

XenDesktop Explorer Monday, April 25, 2016 10:25 PM - 2:25 AM 4 hours | Reports

Session: XDA\win7Static013(Xen Desktop2)

Summary Monitor Desktop Storage User Host Dependency Processes

Resource Utilizations

CPU Load

CPU Utilization: 17 %

Network I/O

Network Utilization: 10 Mb/s

Memory

Memory Utilization: 85 %

Datstore I/O

Datstore Utilization: 0.03 MB/s

Virtual Machines at 10.30.169.38

Virtual Machine Name	Status	CPU	Memory	Host Name	Host Status
win2012	✓	n/a	n/a	10.30.169.38	✓
win2k8001	⚠	2.7 %	8.0 %	10.30.169.38	✓
win2k8Template	⚠	n/a	n/a	10.30.169.38	✓
win7Sp1Template	✖	0.1 %	4.0 %	10.30.169.38	✓
win7Static011	✓	n/a	n/a	10.30.169.38	✓
win7Static012	⚠	3.2 %	9.0 %	10.30.169.38	✓
win7Static013	⚠	4.0 %	15.0 %	10.30.169.38	✓

Sessions

Type	User	Client	Desktop	Session Details	Processes	Remote Latency	Explorer
Desktop	桌面用户1	ZHUVMD76DEMO(10.30.168.172)	win2k8001.xda.local	View Session	View Details	View Details	Explorer
Desktop	桌面用户1	ZHUVMD76DEMO(10.30.168.172)	win7Static012.xda.local	View Session	View Details	View Details	Explorer
Application	Xen Desktop2	ZHUVMD76DEMO(10.30.168.172)	win7Static013.xda.local	View Session	View Details	View Details	Explorer

Table 19. XenDesktop Explorer: Host tab

Resource Utilizations

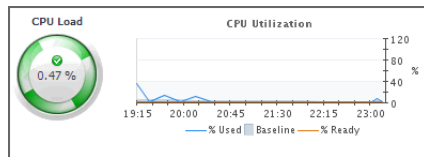
The **CPU Load** spinner indicates the current percentage of the selected virtual machine's CPU load, used to execute system code and user programs, based on the total CPU capacity.

The **% Used** line in the **CPU Utilization** chart shows the percentage of the CPU utilization used by the virtual machine to execute system code and user programs, during the selected time period.

% Ready displays the percentage of the virtual machine's CPU resources that are ready to execute system code and user programs during the selected time period.

CPU Load

The **Baseline** area in the chart indicates the expected CPU utilization range based on historical data.

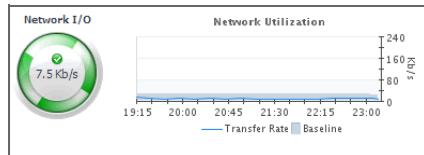


The **Network I/O** spinner indicates the current rate at which the selected virtual machine transfers data from and to the network.

The **Transfer Rate** line in the **Network Utilization** chart shows the rate at which the selected virtual machine receives and sends data to the network during the selected time period.

The **Baseline** area in the chart indicates the expected network utilization range based on historical data.

Network I/O

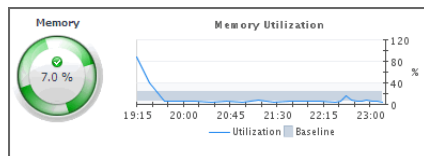


The **Memory** spinner indicates the current percentage of the average memory usage by the selected virtual machine, based on the total memory capacity.

The **Utilization** line in the **Memory Utilization** chart shows the percentage of memory used by the virtual machine during the selected time period.

The **Baseline** area in the chart indicates the expected memory utilization range based on historical data.

Memory



The **Datastore I/O** spinner indicating the current datastore I/O rate the selected virtual machine utilizes, based on the total datastore capacity.

The **Transfer Rate** line in the **Datastore Utilization** chart shows the rate at which the virtual machine reads and writes data to the datastore during the selected time period.

The **Baseline** area in the chart indicates the expected datastore utilization range based on historical data.

Datastore I/O

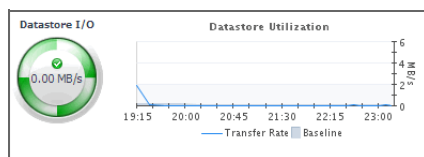


Table 19. XenDesktop Explorer: Host tab

Virtual Machines

Name The name of the virtual machine

Virtual Machine

Status The current alarm severity of the virtual machine.

CPU A sparkline indicating the percentage of the CPU utilization used by the virtual machine to execute system code and user programs, during the selected time period.

Host

Name The name of the physical host on which the virtual machine is running.

Status The highest severity of all alarms generated against the physical host on which the virtual machine is running.

General information about the session, such as its type (desktop or application), the user running the session, client name, desktop name, additional session details, resource utilization, and latency.

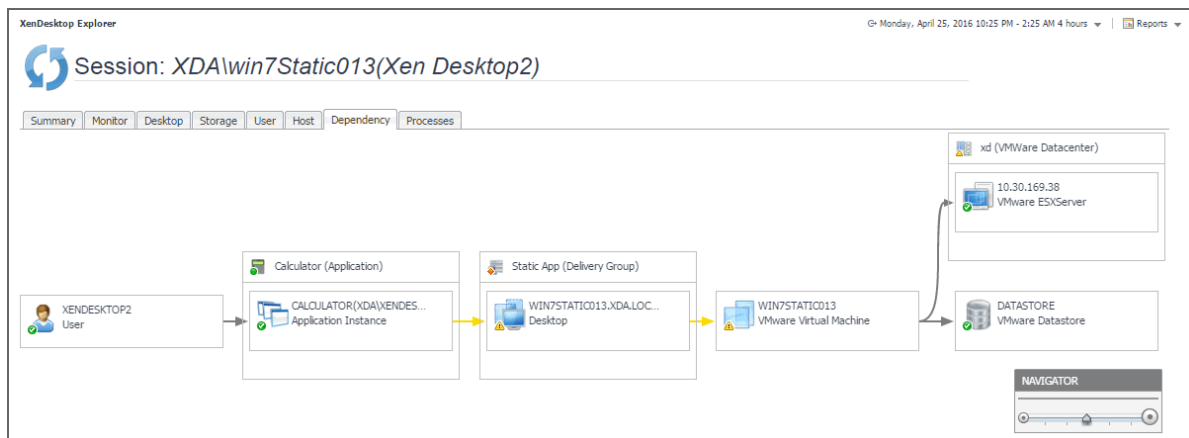
Sessions

Type	User	Client	Desktop	Session Details	Resource Utilization	Remote Latency	Explorer
Desktop	Caprice Juliana	Caprice_Juliana(10.0.0.9)	WIN7002.xda.local	View Session	View Details	View Details	Explorer

Dependency tab

The **Dependency** tab helps you understand the dependencies between the XenDesktop components associated with the selected session. The dependency map displays the relationships between the XenDesktop user, Desktop, virtual machine, datastore, and physical host. For complete information about dependency maps, see [Viewing object dependencies](#) on page 104.

Figure 43. XenDesktop Explorer: Dependency tab



Processes tab

The **Processes** tab displays an organized view of process information for a selected session.

When you select:

- *Application session:* This tab displays the metrics for all processes associated with the session.
- *Desktop session:* This tab displays the metrics for the top consumers of system resources. You can configure the number of top processes that you want to display using the `topN` XenDesktop Agent property.

Use this tab to understand the trends in usage of the process resources, and to look for the signs of compromised performance. For example, high peaks in the memory usage chart, that exceed historical values could result in performance degradation and should be investigated.

If there are any processes that you do not want to monitor, you can add them to the `Process Black List` in the XenDesktop Agent properties.

For more information about the `topN` and `Process Black List` agent properties, see [Configuring XenDesktop Agent Process Configuration properties](#) on page 23.

Figure 44. XenDesktop Explorer: Processes tab

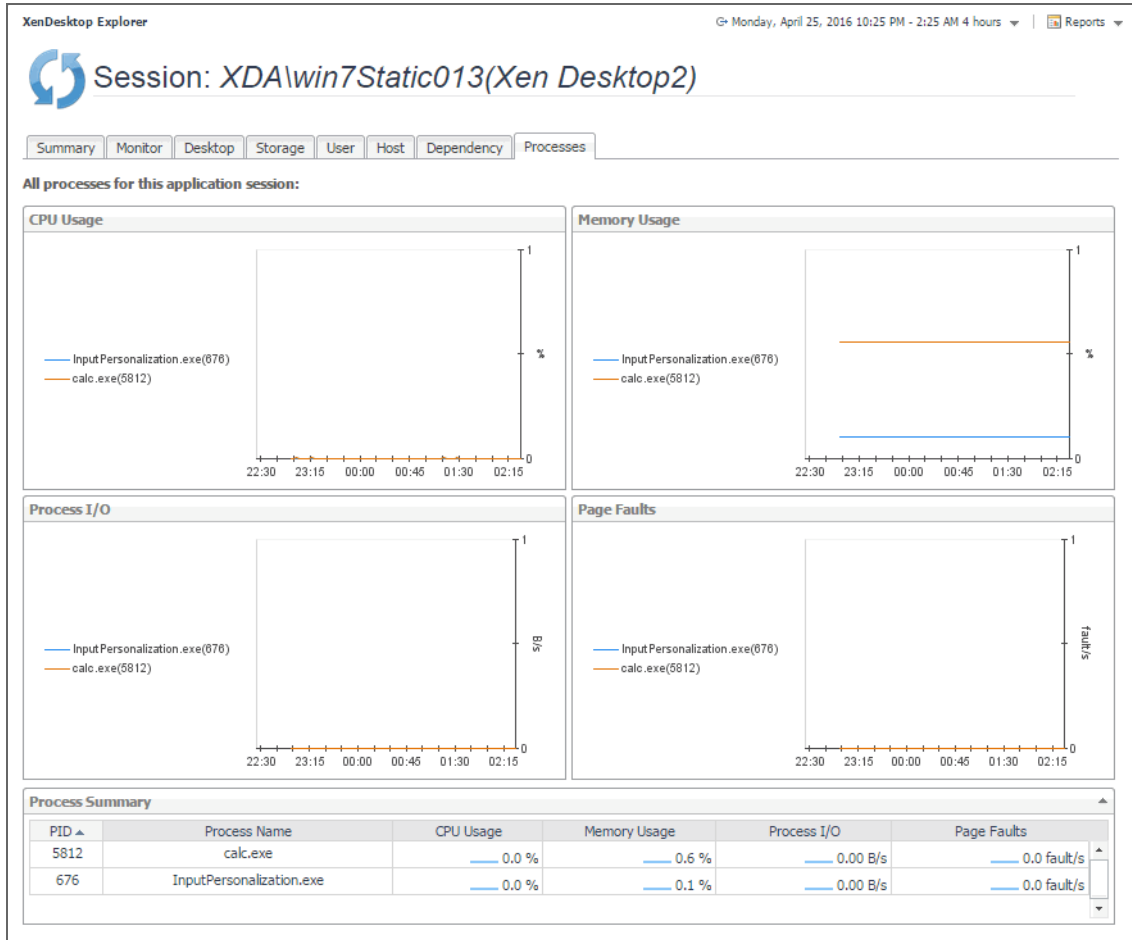
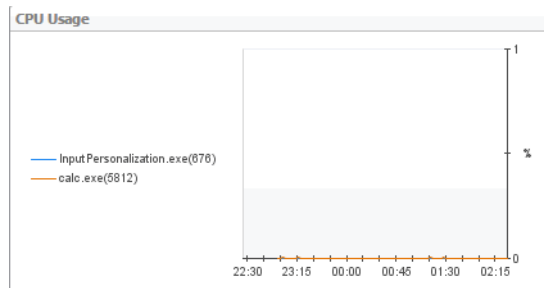


Table 20. XenDesktop Explorer: Processes tab

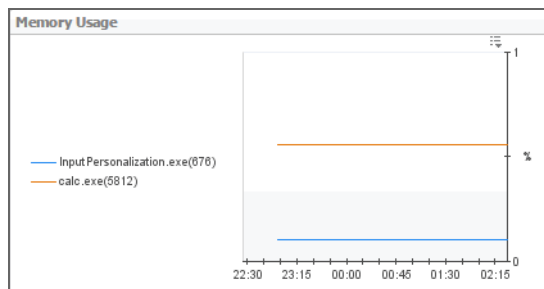
For each identified process, the **CPU Usage** chart displays the percentage of CPU resources used by the process during the selected time period.

CPU Usage



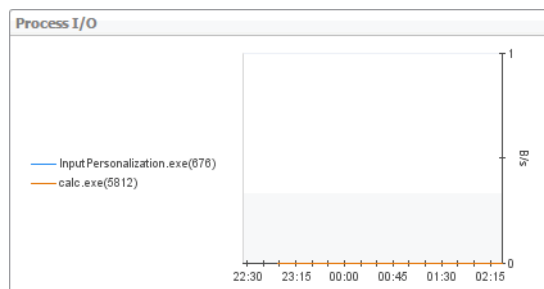
For each identified process, the **Memory Usage** chart displays the percentage of memory resources that are in use, during the selected time period.

Memory Usage



For each identified process, the **Process I/O** chart displays its data transfer rates, during the selected time period.

Process I/O



For each identified process, the **Page Faults** chart displays the number of page faults encountered each second, during the selected time period.

Page Faults

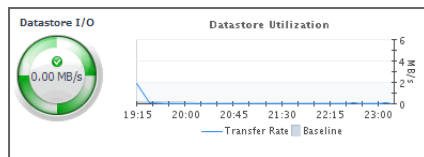


Table 20. XenDesktop Explorer: Processes tab

Metrics collected about each identified process.

Process Summary						
PID	Process Name	CPU Usage	Memory Usage	Process I/O	Page Faults	
5812	calc.exe	0.0 %	0.6 %	0.00 B/s	0.0 fault/s	
676	InputPersonalization.exe	0.0 %	0.1 %	0.00 B/s	0.0 fault/s	

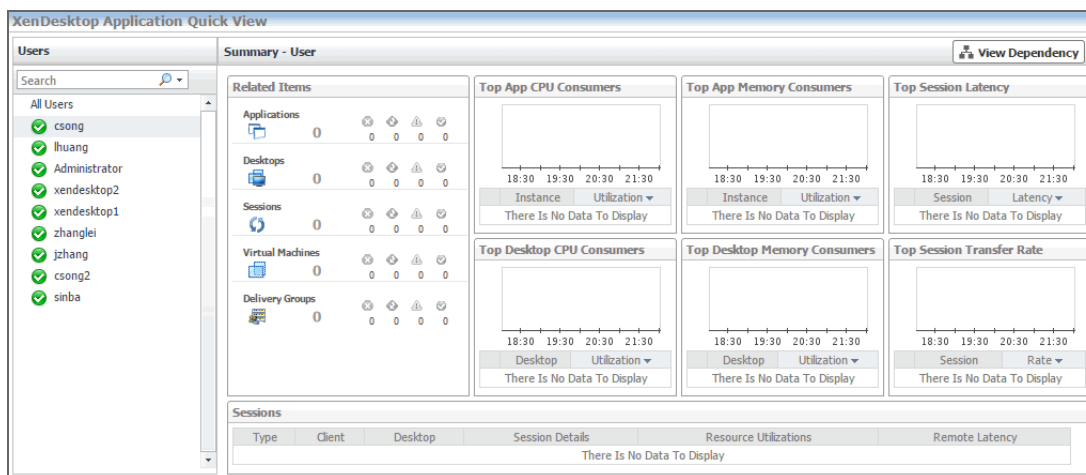
Process Summary

- PID** The process ID.
- Name** The name of the process.
- CPU Usage** The percentage of CPU resources the process currently uses.
- Memory Usage** The percentage of memory resources the process currently uses.
- Process I/O** The I/O data transfer rates for the process.
- Page Faults** The number of page faults the process encounters per second.

Monitoring Users

XenDesktop® facilitates delivery of application components to end users on demand. Foglight™ for Citrix XenDesktop and XenApp allows you to monitor the over utilization of resources associated with XenDesktop users. The information appearing in the **XenDesktop User Quick View** can help you discover potential resource-level issues that can be caused by higher than usual CPU or memory usage, or increasing latency and session rates, and to reallocate resources where they are most needed.

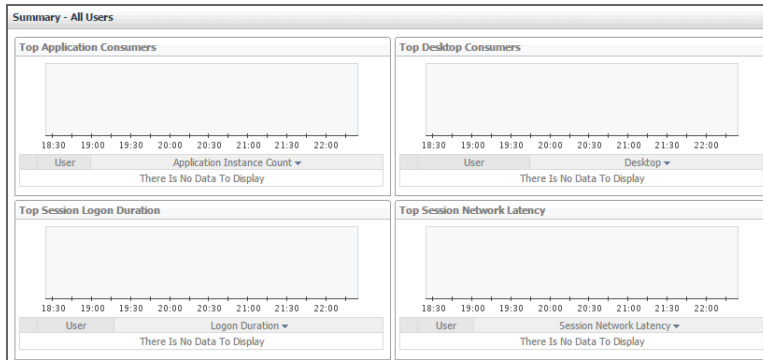
Figure 45. XenDesktop Users Quick View



To explore Users:

- 1 On the navigation panel, under **Dashboards**, click **XenDesktop Environment**.
- 2 On the XenDesktop Environment dashboard, on the **Monitoring** tab, click the **Users** tile.
- 3 In the **XenDesktop Users Quick View**, in the **Users** view on the left, click **All Users**.

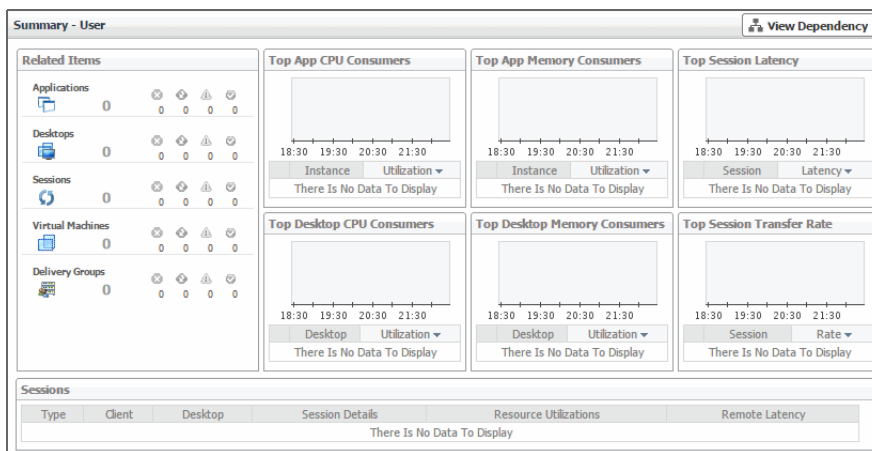
The **XenDesktop Users Quick View** refreshes, showing the **Summary - All Users** view on the right.



This view identifies the applications with the highest number of instances, and the highest CPU and memory utilization, and session latency. For more information, see [Identifying top consumers](#) on page 89.

- 4 In the **XenDesktop Users Quick View**, in the **Users** view on the left, click a user node.

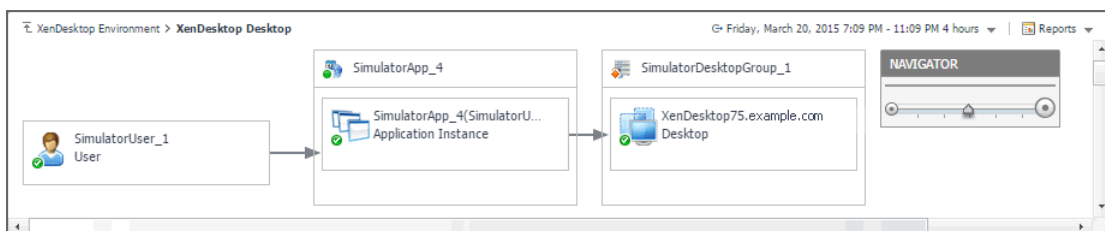
The **XenDesktop Users Quick View** refreshes, showing the **Summary - User** view on the right.



This view displays a summary about XenDesktop objects associated with the selected user and shows the levels of CPU and memory utilization associated with desktops and applications. For more information, see [Investigating the levels of resource consumption](#) on page 90.

- 5 If you want to view the relationship of the selected User object with other components in your integrated environment, in the top-right corner, click **View Dependency**.

The display area refreshes, showing a dependency map.



The map illustrates how the selected User object relates to other components in your monitored environment. For more information, see [Viewing object dependencies](#) on page 104.

i **TIP:** To return to the XenDesktop Environment dashboard, use the bread crumb trail in the top-left corner.

Identifying top consumers

Your monitored XenDesktop environment delivers applications to end users on demand. The **Summary - All Users** view identifies the users with the highest applications and desktop usage, longest logon times, and highest network latencies. This view appears in the Quick View when you select **All Users** in the **Users** view on the left. Use it to look for potential bottlenecks in your system in order to prevent potential service disruptions by reallocating system resources where they are most needed.

Figure 46. Summary - All Users view

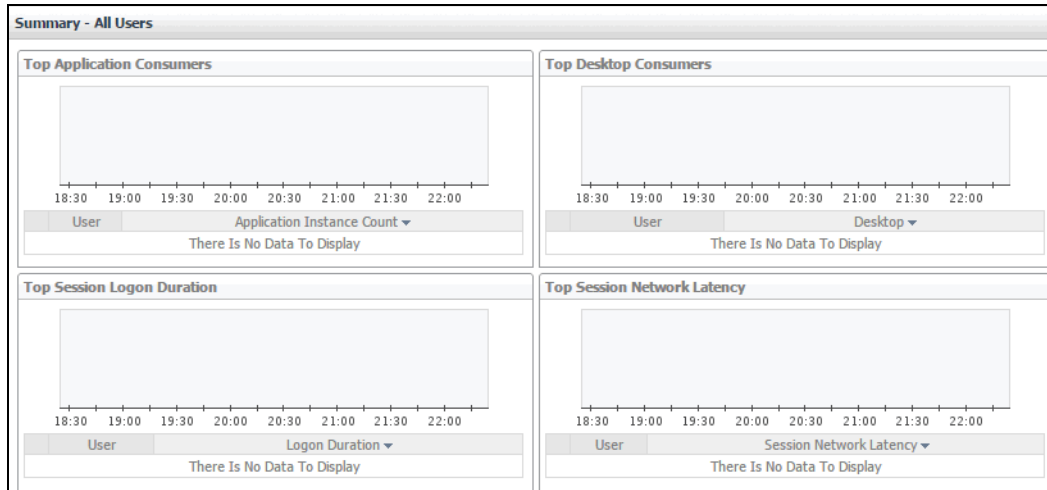
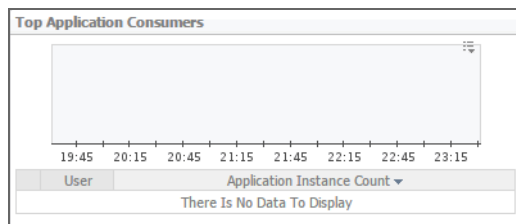


Table 21. Summary - All Users view

The users running the most application instances over the selected time range.

Top Application Consumers



The users running the most desktop instances over the selected time range.

Top Desktop Consumers

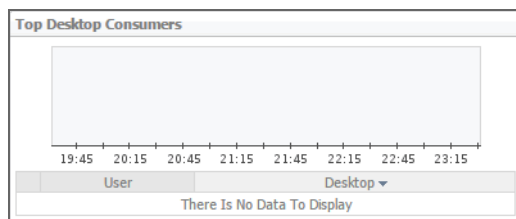
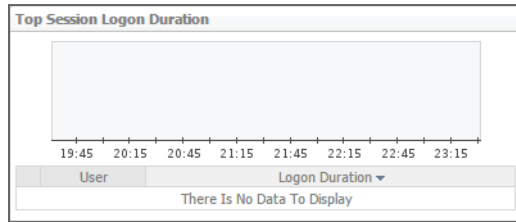


Table 21. Summary - All Users view

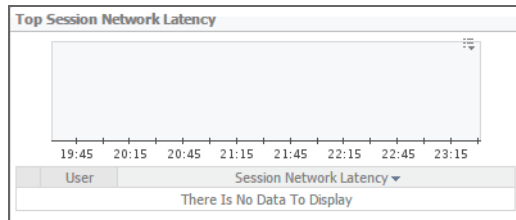
The users running the sessions with the longest logon duration over the selected time range.

Top Session Logon Duration



The users running the sessions with the highest network latency, over the selected time range.

Top Session Network Latency



Investigating the levels of resource consumption

Your monitored XenDesktop® environment delivers virtual desktops and applications are delivered to end users on demand. You can review the levels of CPU and memory resources consumed by these elements, along with session-related metrics in the **Summary - User** view. Use it to identify the applications and desktops that consume the highest amounts of CPU and memory resources, and to look more closely at session latency and transfer rates. An application or desktop with consistently low CPU or memory utilization rates, for example, often calls for re-allocating these under used resources where they are more needed.

Figure 47. Summary - User view

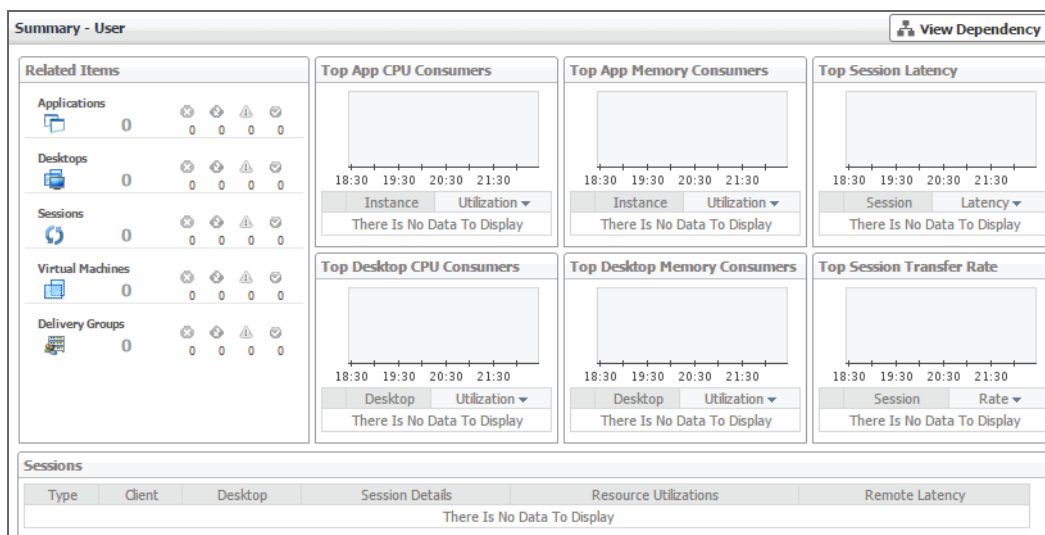
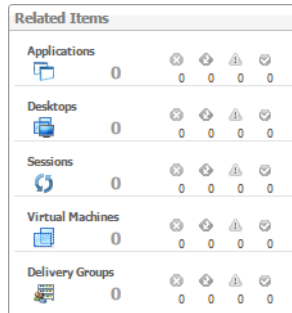


Table 22. Summary - User view

The objects that are associated with the selected user object and their alarm state.

Figure 48. Related Items view

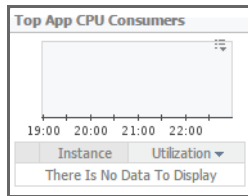
Related Items



The application instances associated with the selected user that are consuming the highest amounts of CPU resources, over the selected time range.

Figure 49. Top App CPU Consumers view

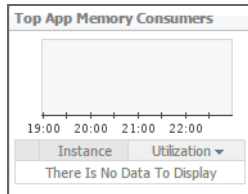
Top App CPU Consumers



The application instances associated with the selected user that are consuming the highest amounts of memory resources, over the selected time range.

Figure 50. Top App Memory Consumers view

Top App Memory Consumers



The sessions initiated by the selected user that have the highest latency, over the selected time range.

Figure 51. Top Session Latency view

Top Session Latency

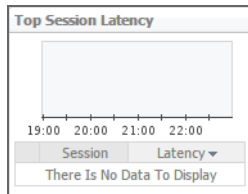
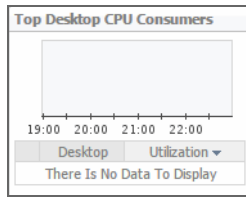


Table 22. Summary - User view

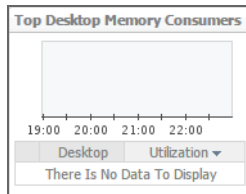
The desktop instances associated with the selected user that are consuming the highest amounts of CPU resources, over the selected time range.

Top Desktop CPU Consumers



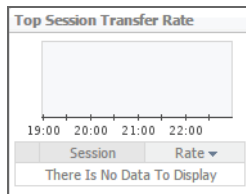
The desktop instances associated with the selected user that are consuming the highest amounts of memory resources, over the selected time range.

Top Desktop Memory Consumers



The sessions initiated by the selected user that have the highest network transfer rates, over the selected time range.

Top Session Transfer Rate



General information about the sessions initiated by the selected user, such as the session type, client name, desktop name, additional session details, resource utilization, and latency.

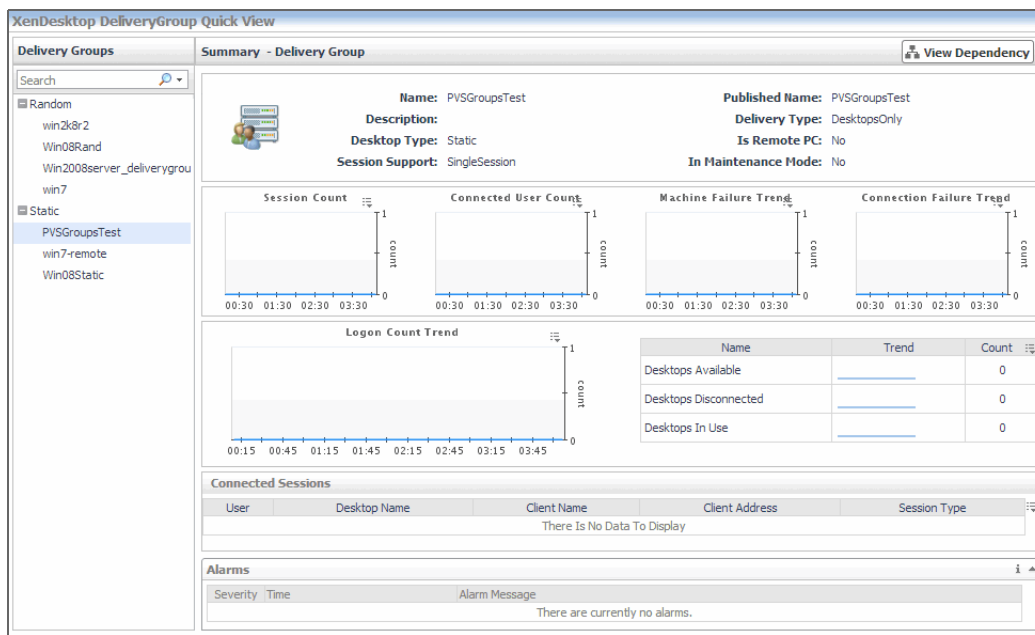
Sessions

Sessions					
Type	Client	Desktop	Session Details	Resource Utilizations	Remote Latency
There Is No Data To Display					

Monitoring Delivery Groups

A Delivery Group specifies which users can access desktops or applications based on their user type. You can monitor the performance of Delivery Groups when you select the **Delivery Groups** tile on the XenDesktop Environment dashboard. The information appearing in the **XenDesktop DeliveryGroup Quick View** can help you discover sources of performance degradation such as high number of sessions or machine failures, and to reallocate resources where they are most needed.

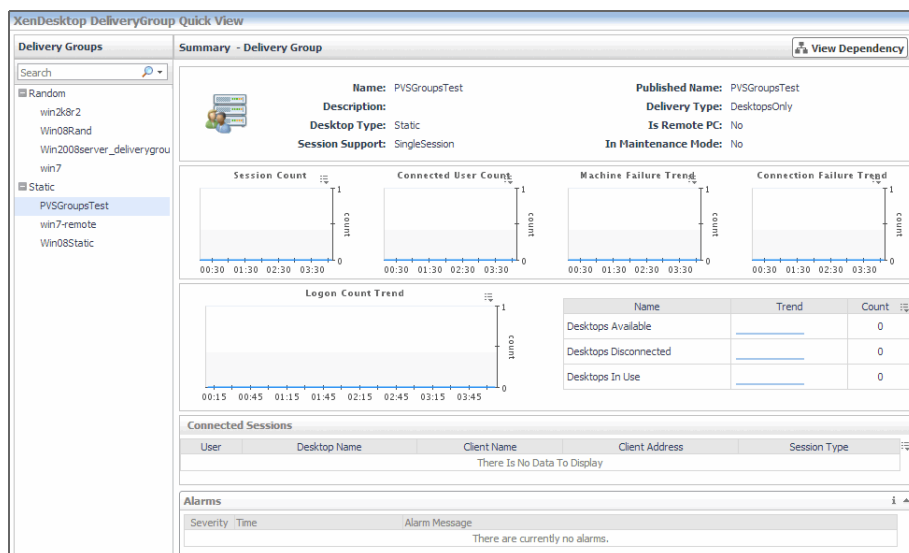
Figure 52. XenDesktop DeliveryGroup Quick View



To explore Delivery Groups:

- 1 On the navigation panel, under **Dashboards**, click **XenDesktop Environment**.
- 2 On the XenDesktop Environment dashboard, on the **Monitoring** tab, click the **Delivery Groups** tile.
- 3 In the **XenDesktop DeliveryGroup Quick View**, in the **Delivery Groups** view on the left, click a delivery group node.

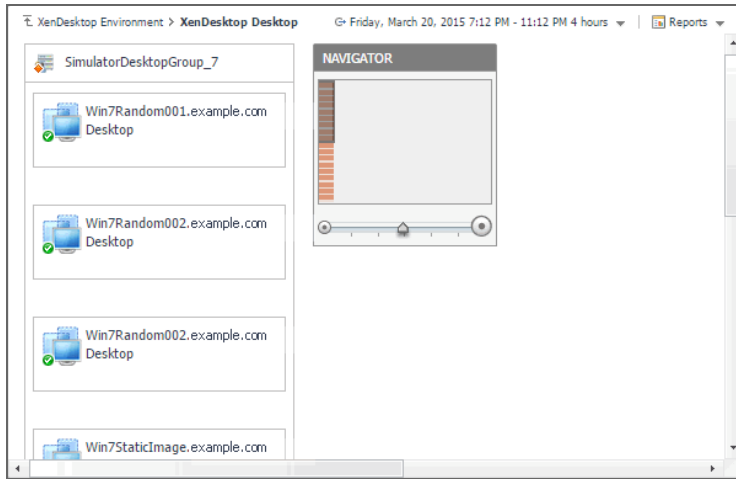
The **XenDesktop DeliveryGroup Quick View** refreshes, showing the **Summary - Application** view on the right.



This view displays general information about the selected delivery group and shows the high-level performance trends in session counts, logon duration, machine and connection failures, and so on. For more information, see [Investigating Delivery Group details](#) on page 94.

- 4 If you want to view the relationship the selected Delivery Group has with other components in your integrated environment, in the top-right corner, click **View Dependency**.

The display area refreshes, showing a dependency map.



The map illustrates how the selected Delivery Group relates to other components in your monitored environment. For more information, see [Viewing object dependencies](#) on page 104.

TIP: To return to the XenDesktop Environment dashboard, use the breadcrumb trail in the top-left corner.

Investigating Delivery Group details

In your monitored environment, a Delivery Group is a collection of desktops and applications that can be accessed by specific end users. You can review the performance of individual Delivery Groups in the **Summary - Delivery Group** view. This view allows you to review general information about a selected delivery group along with performance trends in session counts, connected users, machine and connection failures. Use this view to review the general trends in the overall performance of monitored Delivery Groups and to look for any indicators that suggest potential bottlenecks. For example, an unusually high number of connection failures can affect the end-user experience and should be investigated.

Figure 53. Summary - Delivery Group view

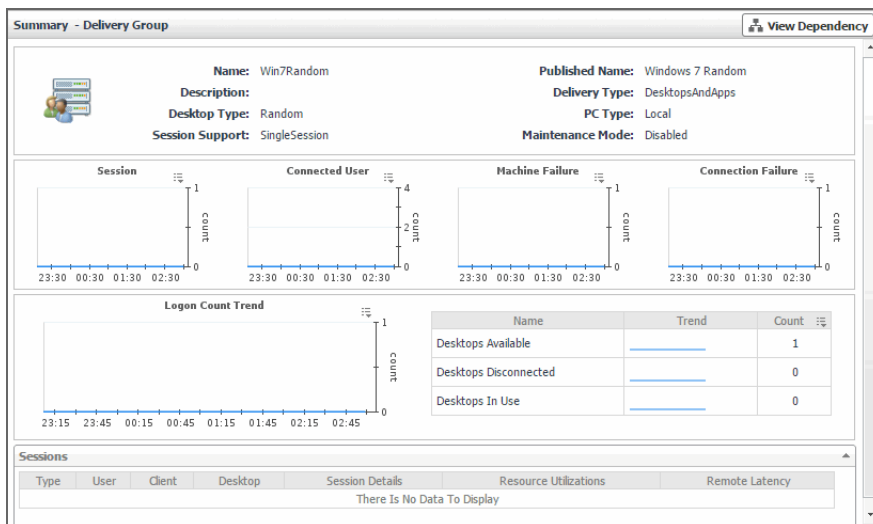


Table 23. Summary - Delivery Group view

General information about the session, such as its name, state, catalog name, type (desktop or application), support type, and the delivery group to which it belongs.

General information

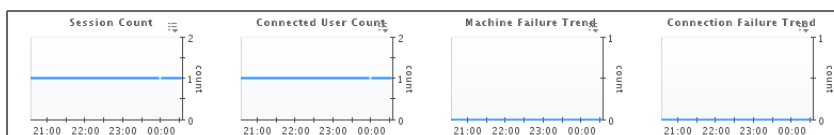
	Name: win7-remote	Published Name: win7-remote
	Description: win7-description	Delivery Type: DesktopsOnly
	Desktop Type: Static	Is Remote PC: Yes
	Session Support: SingleSession	In Maintenance Mode: No

**Session Count
Connected User
Count**

Session and user counts, and the counts of system- and connection-related failures, all over the selected time period.

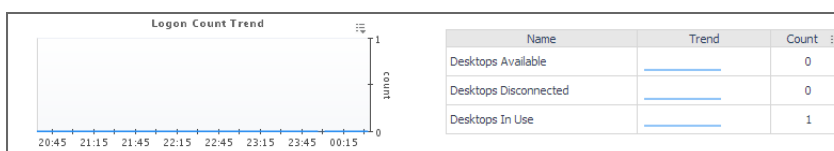
**Machine Failure
Trend**

**Connection
Failure Trend**



Displays user logon counts over the selected time period. It also lists the numbers of desktops that are available, disconnected, and in use, and the projected trends.

**Logon Count
Trend**



General information about the session, such as its type (desktop or application), the user associated with the session, client name, desktop name, additional session details, resource utilization, and latency.

Sessions

Type	User	Client	Desktop	Session Details	Resource Utilization	Remote Latency	Explorer
	Caprice Juliana	Caprice_Juliana(10.0.0.9)	WIN7002.xda.local	View Session	View Details	View Details	Explorer

Displays the alarms generated against the selected delivery group. Each entry indicates the alarm severity (Warning, Critical, or Fatal), the time when the alarm was generated, and an explanation indicating what triggered the alarm.

Alarms

Severity	Time	Alarm Message
	5/20/14 3:07 PM	Connected user count exceeded the normal limits. XenDesktop DeliveryGroup win7-remote's connected user count 1 exceeded t
	5/20/14 3:07 PM	Session count exceeded the normal limits. XenDesktop DeliveryGroup win7-remote's session count 1 exceeded the normal limits.

Monitoring vSphere resources

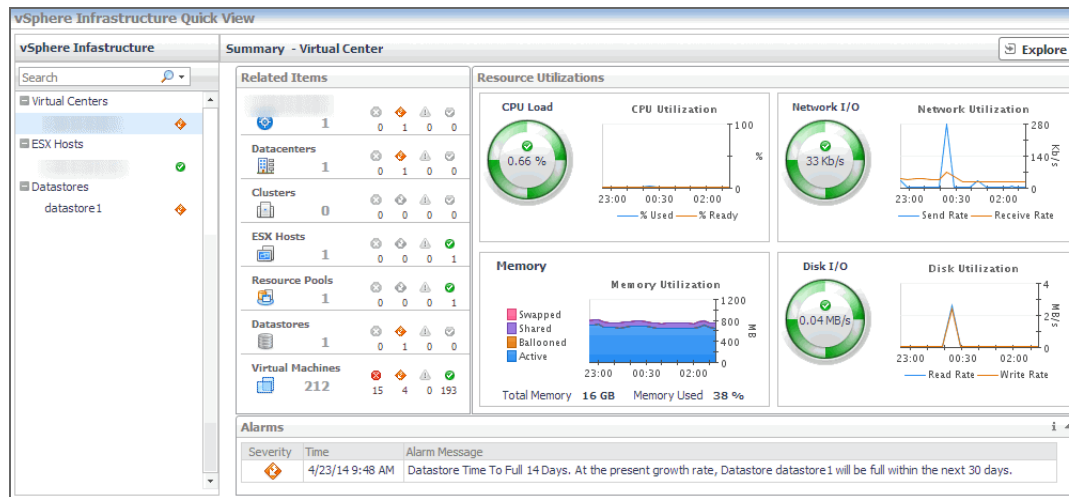
A typical vSphere® infrastructure consists of the following objects:

- **Virtual centers:** Software used to manage virtual environments that are built on the VMware® virtualization platform. Each virtual center creates a hierarchical structure of virtual objects that enables a system administrator to logically lay out their virtual infrastructure configuration.
- **ESX® hosts:** Physical machines hosting one or more virtual machines.
- **Datastores:** Storage location for virtual machine files.

i IMPORTANT: vSphere resources are monitored with Foglight™ for VMware. The VMware Performance Agent, included with Foglight for VMware, collects this information and populates the XenDesktop Environment dashboard. If you want to monitor a Virtual Center, you need a running instance of the VMware Performance Agent. For more information about this agent, see the *Foglight for VMware User and Reference Guide*.

You can monitor the performance of these elements when you select the **vSphere** tile on the XenDesktop Environment dashboard. The information appearing in the **vSphere Infrastructure Quick View** can help you discover sources of performance degradation such as spikes in CPU, memory and disk usage, and to reallocate resources where they are most needed.

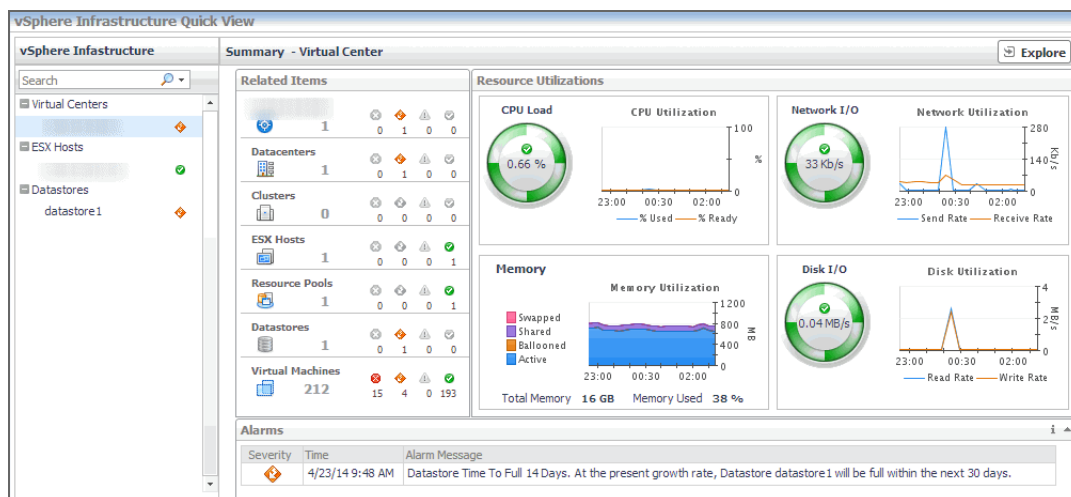
Figure 54. vSphere Infrastructure Quick View



To explore vSphere resources:

- 1 On the navigation panel, under **Dashboards**, click **XenDesktop Environment**.
- 2 On the XenDesktop Environment dashboard, on the **Monitoring** tab, click the **vSphere** tile.
- 3 To display resource utilization statistics for a monitored virtual center or an ESX host, **vSphere Infrastructure Quick View**, in the **vSphere Infrastructure** view on the left, click a virtual center node or an ESX host node.

The **vSphere Infrastructure Quick View** refreshes, showing a summary view on the right.

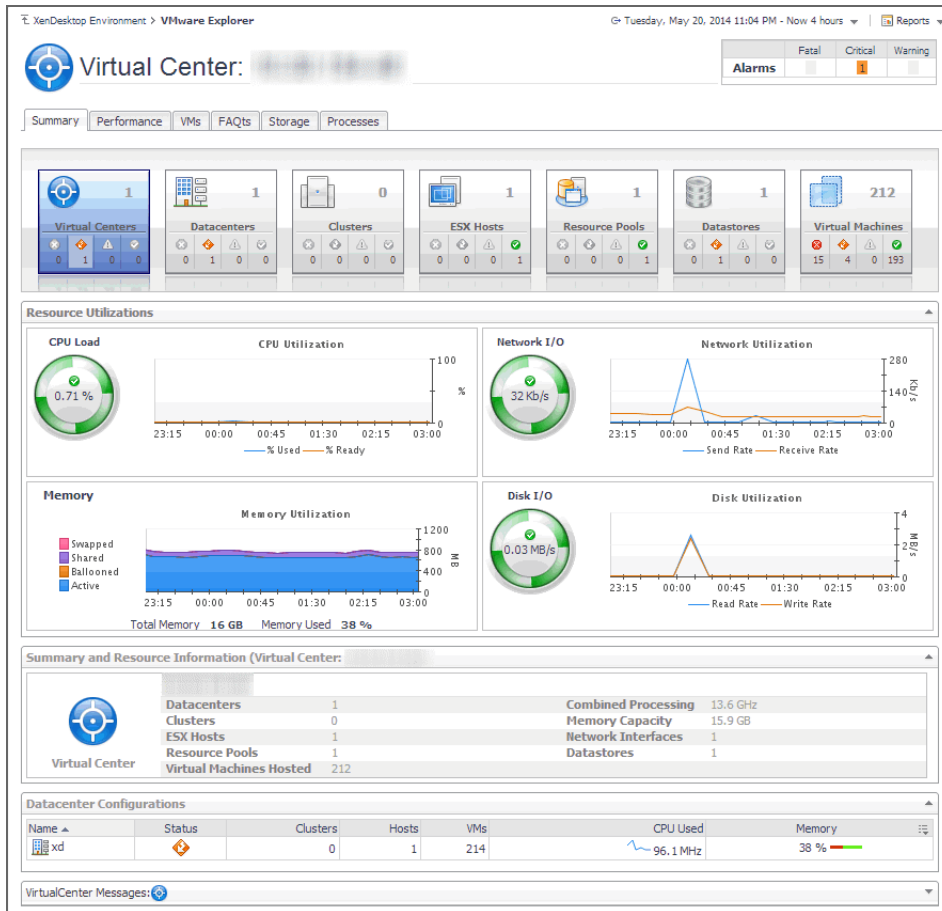


This view displays the overall resource utilization for the selected object and shows the high-level performance trends in the CPU, memory, disk, and network utilization. For more information, see [Investigating the use of Virtual Center and ESX Host resources](#) on page 98.

- 4 To display more details about the selected object, in the top-right corner, click **Explore**.

The display area refreshes, displaying information about the selected object in the VMware Explorer. This dashboard provides a hierarchical inventory, in the form of tiles, of the objects that are related to the

selected object. It also contains a set of collapsible views, displaying resource utilization metrics, physical configuration details, datastore configuration, and a list of messages associated with the virtual center.

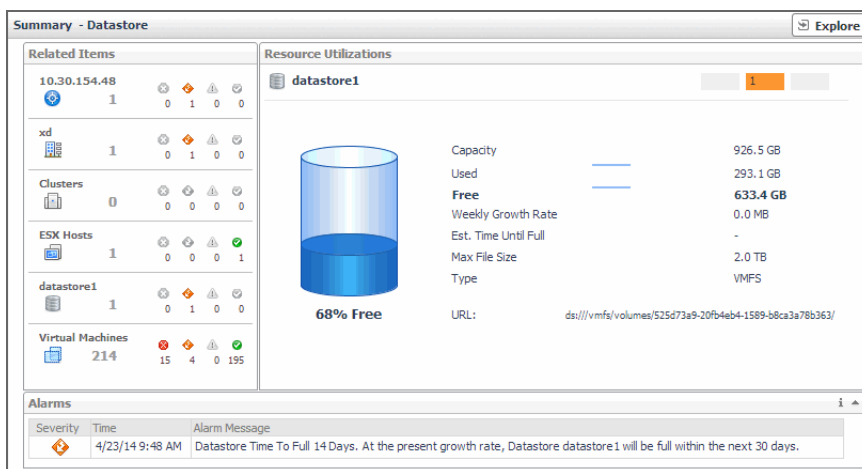


The VMware Explorer dashboard comes with Foglight for VMware. For more information about this dashboard, see the *Foglight for VMware User and Reference Guide*.

TIP: To return to the XenDesktop Environment dashboard, use the bread crumb trail in the top-left corner.

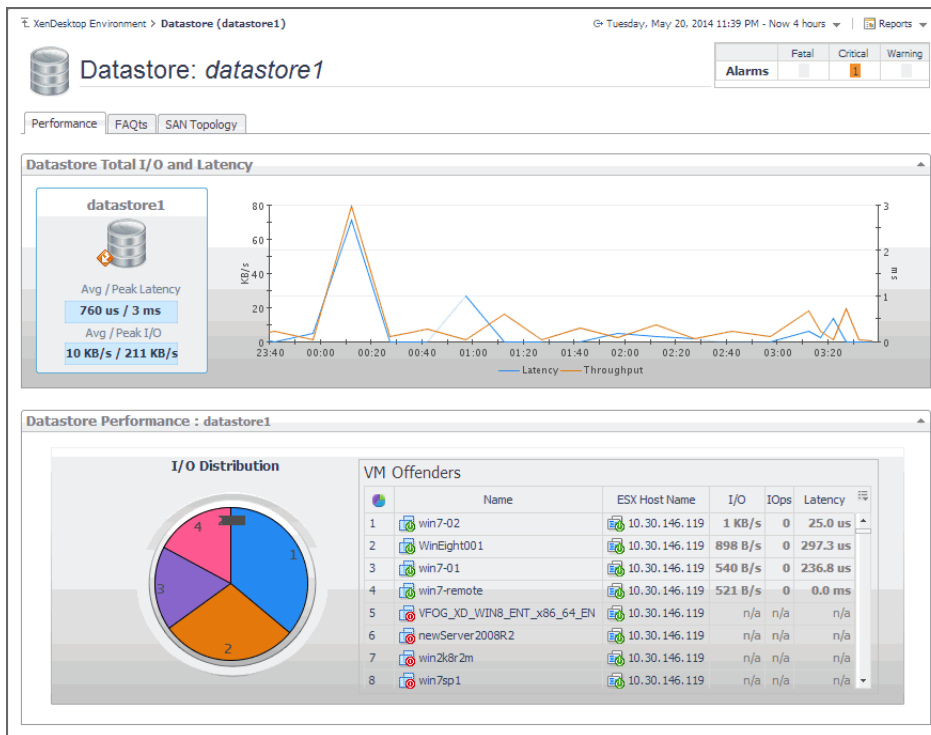
- In the **vSphere Infrastructure Quick View**, in the **vSphere Infrastructure** view on the left, under **Datastores**, click a datastore node.

The **vSphere Infrastructure Quick View** refreshes, showing the **Summary - Datastore** view on the right.



This view displays the overall resource utilization and the amounts of system resource consumption for the selected physical datastore. For more information, see [Investigating the use of Datastore resources](#) on page 101.

- To display more details about the selected datastore, in the top-right corner, click **Explore**.



The display area refreshes, showing additional information about the selected datastore. This view provides disk storage performance metrics for the selected datastore. For more information, see [Exploring individual Datastores](#) on page 103.

TIP: To return to the XenDesktop Environment dashboard, use the bread crumb trail in the top-left corner.

Investigating the use of Virtual Center and ESX Host resources

A virtual center application creates a hierarchical structure of virtual objects that enables a system administrator to logically lay out their virtual infrastructure configuration. In your monitored virtual center, ESX[®] hosts are physical machines hosting one or more virtual machines.

You can review the performance of monitored virtual centers and ESX hosts using the **Summary - Virtual Center** and **Summary - ESX Host** views. These views can help you identify and prevent potential bottlenecks by reallocating resources where they are most needed. They appear on the right in the Quick View when you select a virtual center or an ESX host in the left pane.

Figure 55. Summary - ESX Host view

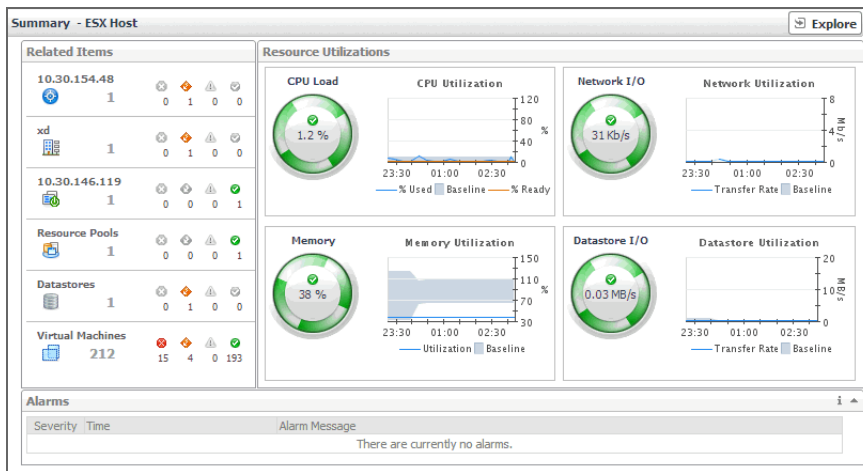
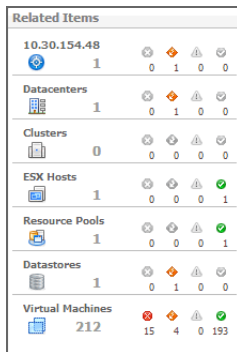


Table 24. Summary - ESX Host view

Identifies the objects that are associated with the virtual center or ESX host and displays their alarm state.

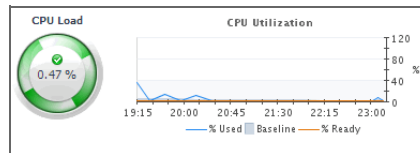
Related Items



Resource Utilizations

CPU

The **CPU Load** spinner indicates the current percentage of the CPU resources the selected virtual center or ESX host uses to execute system code and user programs, based on the total CPU capacity. The **% Used** line in the **CPU Utilization** chart shows the percentage of the CPU resources the selected virtual center or ESX host uses to execute system code and user programs, during the selected time period. **% Ready** displays the percentage of the CPU resources that are ready for the virtual center or ESX host to execute system code and user programs during the selected time period. The **Baseline** area in the chart (ESX hosts only) indicates the expected CPU utilization range based on historical data.



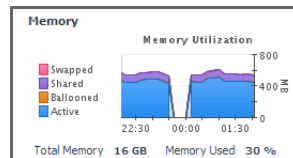
Virtual Centers only

Table 24. Summary - ESX Host view

The **Swapped** line in the **Memory Utilization** chart shows the amount of memory that is stored in disk swap space, during the selected time period. **Shared** displays the amount of the virtual machine memory that is freed up due to transparent page sharing. **Ballooned** represents the amount of physical memory that is actively being used by the VMware Memory Control Driver to allow the guest OS to selectively swap memory. **Active** shows the amount of the available memory that the virtual center uses during the selected time period.

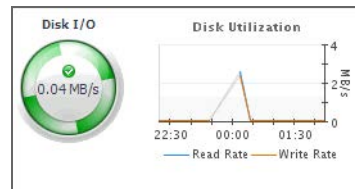
Memory

The **Total Memory** value below the chart is the total amount of memory available to the selected virtual center. **Memory Used** shows the percentage of the memory resources the selected virtual center currently uses



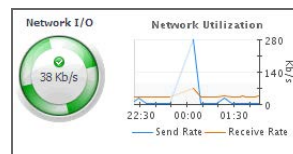
The **Disk I/O spinner** indicates the rate at which the selected virtual center currently reads data from and writes to disk. The **Read Rate** line in the **Disk Utilization** chart represents the rate at which the selected virtual center reads data from the disk during the selected time period. **Write Rate** displays the rate at which the selected virtual center writes data to disk.

Disk



The **Network I/O spinner** indicates the rate at which the selected virtual center currently reads data from and writes to the network. The **Receive Rate** line in the **Network Utilization** chart represents the rate at which the selected virtual center reads data from the network during the selected time period. **Send Rate** displays the rate at which the selected virtual center sends data to the network.

Network



ESX hosts only

The **Memory Load spinner** indicates the percentage of the memory resources the selected ESX host currently uses. The **Utilization** line in the **Memory Utilization** chart shows the percentage of the memory resources the selected ESX host uses during the selected time period. The **Baseline** area in the chart indicates the expected memory utilization range based on historical data.

Memory

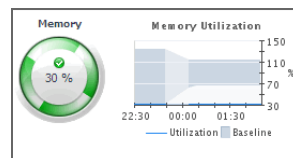
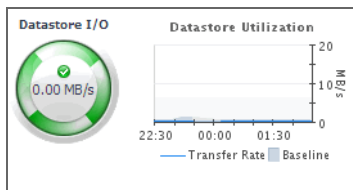


Table 24. Summary - ESX Host view

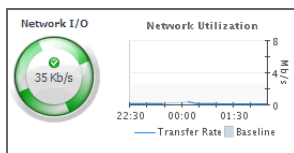
The **Datastore I/O** spinner indicates the rate at which the selected ESX host currently reads data from and writes to the associated datastore. The **Transfer Rate** line in the **Datastore Utilization** chart represents the rate at which the selected virtual center reads data from and writes data to the datastore during the selected time period. The **Baseline** area in the chart indicates the expected datastore utilization range based on historical data.

Datastore



The **Network I/O spinner** indicates the rate at which the selected ESX host currently reads data from and writes to the network. The **Transfer Rate** line in the **Network Utilization** chart represents the rate at which the selected virtual center transfers data from and to the network during the selected time period. The **Baseline** area in the chart indicates the expected network utilization range based on historical data.

Network



Displays the alarms generated against the selected virtual center or ESX host. Each entry indicates the alarm severity (Warning, Critical, or Fatal), the time when the alarm was generated, and an explanation indicating what triggered the alarm.

Alarms

Severity	Time	Alarm Message
	4/23/14 9:48 AM	Datastore Time To Full 14 Days. At the present growth rate, Datastore datastore1 will be full within the next 30 days.

Investigating the use of Datastore resources

A datastore represents a storage location for virtual machine files. You can review the performance of monitored datastores using the **Summary - Datastore** view, appearing on the right in the **vSphere Infrastructure Quick View**, when you select a datastore in the **vSphere Infrastructure** view on the left. This view displays the overall resource utilization statistics and the amounts of system resource consumption for a physical datastore. This information can help you identify prevent potential bottlenecks. For example, a high amount of used space typically calls for reallocation of storage resources, as required.

Figure 56. Summary - Datastore view

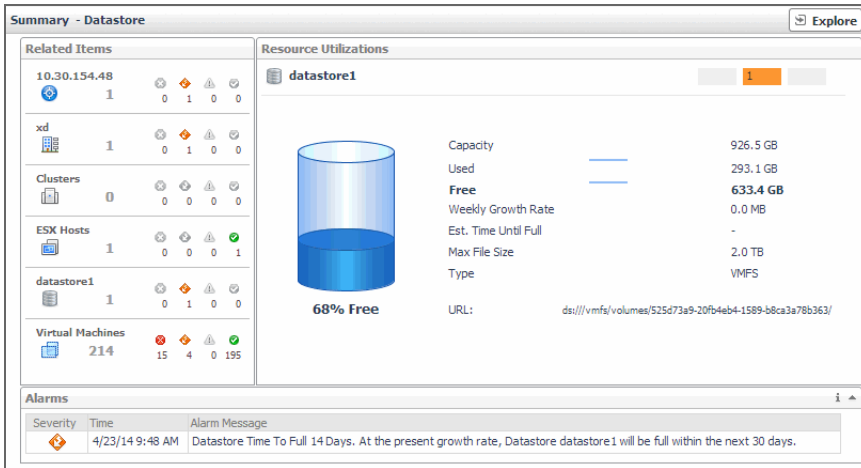
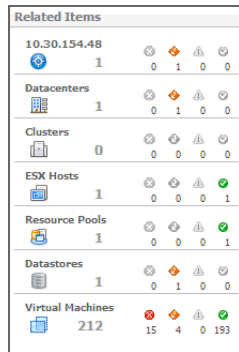


Table 25. Summary - Datastore view

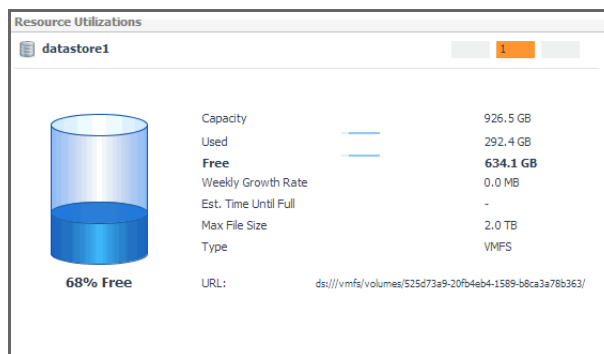
Identifies the objects that are associated with the selected datastore and displays their alarm state.

Related Items



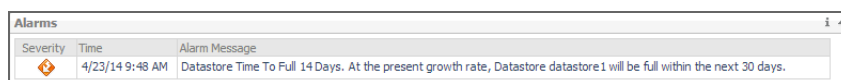
Displays the counts of generated alarms in each severity state, the total disk capacity, amounts of used and free disk space, percentage of free space, estimated weekly rate, estimated time after which the disk will be full, the maximum file size, and file system type.

Resource Utilizations



Displays the alarms generated against the selected datastore. Each entry indicates the alarm severity (Warning, Critical, or Fatal), the time when the alarm was generated, and an explanation indicating what triggered the alarm.

Alarms

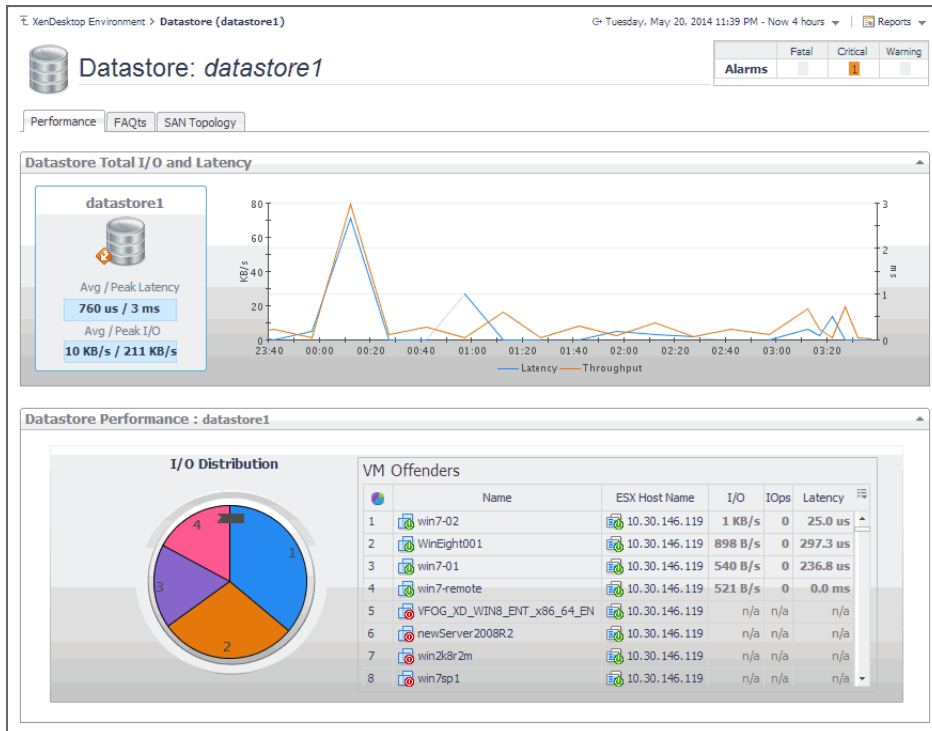


Exploring individual Datastores

If you see any indicators that could lead to datastore performance degradation, you can explore it in more detail. The **Performance** tab on the Datastore Explorer view identifies the virtual machines that consume the highest amounts of the datastore resources. Use it to prevent potential performance bottlenecks by reallocating datastore resources where they are most needed.

The **FAQts** tab on this view allows you to review common questions and answers about the selected datastore. For more information, see [Reviewing Frequently Asked Questions](#) on page 109. The **SAN Topology** tab is provided with Foglight™ for Storage Management. For more information about this tab, see the *Foglight for Storage Management User and Reference Guide*.

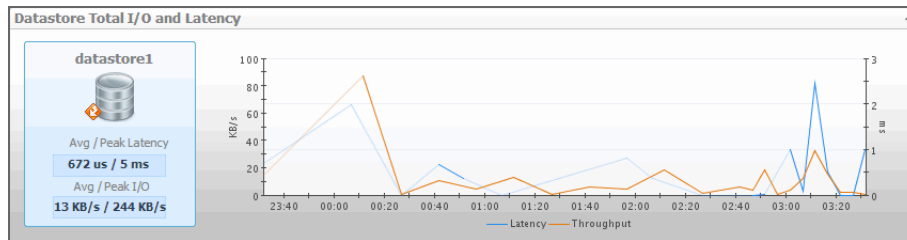
Figure 57. Datastore Explorer



Datastore Explorer

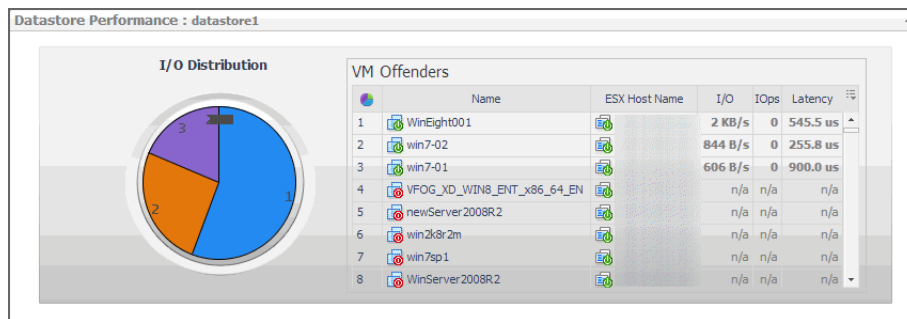
The average disk latency and data transfer rates for the selected datastore.

Datastore Total I/O and Latency



Identifies potential virtual machine offenders that consume the highest amounts of the selected datastore resources. It also displays a pie chart indicating how much the virtual machines associated with the selected datastore contribute to the overall I/O. For each identified virtual machine, it shows its name, the ESX[®] host on which it is running, the disk transfer rate, the rate of I/O operations per second, and the average time that passes between the time the virtual machine issues and executes disk read or write operations.

Datastore Performance



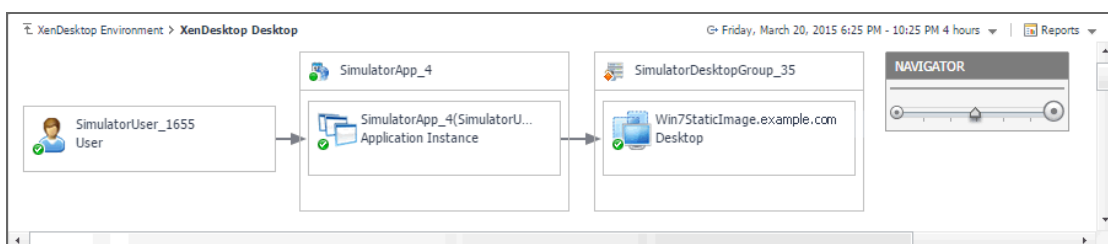
Viewing object dependencies

A typical XenDesktop[®] environment consists of many interrelated components. Understanding the dependencies between logical and virtual components in your monitored environment and the levels of resources they consume allows you to better understand resource-related issues, potentially affecting the stability of your system. This can help you predict the impact a potential outage may have on your environment, and to prevent such events, by reallocating resources where they are most needed.

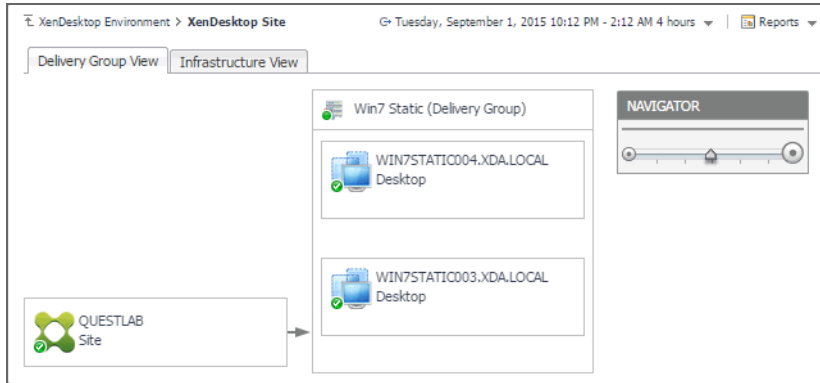
The XenDesktop Dependency dashboard visualizes the relationships between the objects in your environment through an interactive map. The map illustrates how different components relate to each other, and the levels of the available resources available to them.

To access the Dependency map:

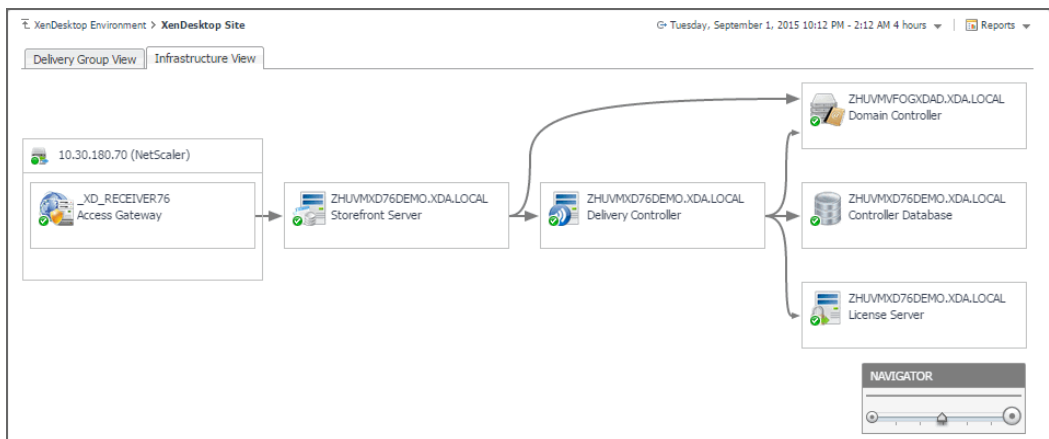
- To view the dependencies associated with a specific delivery group, desktop, application, or with your monitored XenDesktop site, select that component on the XenDesktop Environment dashboard, and click **View Dependency**.



- Alternatively, to see the dependencies associated with your monitored XenDesktop site, on the navigation panel, under **Dashboards**, choose **XenDesktop > XenDesktop Dependency**.
 - Delivery Group View:** A Delivery Group specifies which users can access Desktops or Applications based on their user type. This tab illustrates the relationships between main components associated with the Delivery Groups that belong to the selected XenDesktop site, including the XenDesktop site, any Delivery Groups, and the Desktops and Applications available in these Delivery Groups.



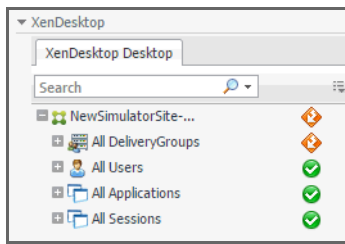
- Infrastructure View:** This tab illustrates the relationships between main infrastructure elements components associated with the Delivery Groups that belong to the selected XenDesktop site, such as the NetScaler Gateway, StoreFront Server, Delivery Controller, Domain Controller Database, and the License Server.



Using dependency maps

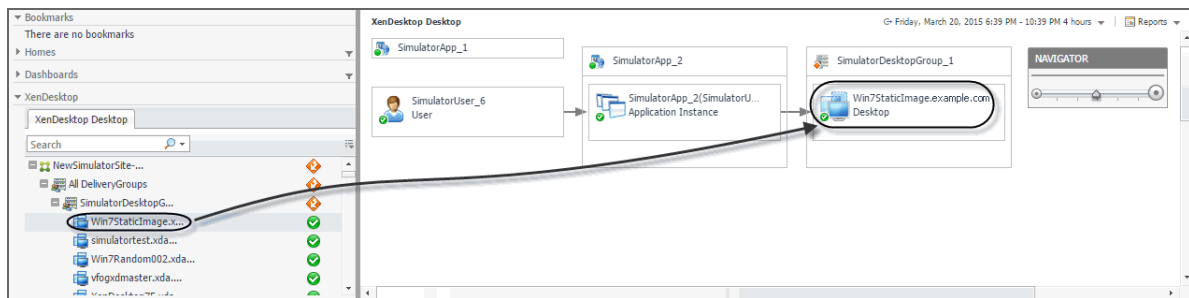
When you open a dependency map, the **XenDesktop Desktop** tab appears on the navigation panel. This tab displays a navigation tree representing a simplified map of your monitored objects. On the right of each object or object group, alarm indicators appear. Each indicator represents the alarm of the highest severity that is generated against the object. For an object type container (for example, **All DeliveryGroups**), the status indicator represents the alarm of highest severity that is outstanding for all objects belonging to that group.

Figure 58. XenDesktop Desktop tab



When you select an object in the navigation tree, the display area refreshes, showing the selected object and any dependencies that it may have with other objects in your monitored environment.

Figure 59. Selecting objects in a dependency map



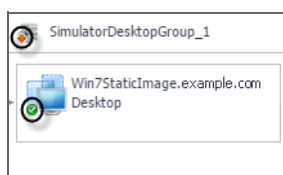
The complexity of the information appearing in a dependency map depends on the selected object and the dependencies that object has with other objects within your integrated infrastructure.

In a large multi-component environment, dependency maps are likely complex and may not fit your screen. The **NAVIGATOR** in the top-right corner allows you to easily set the zoom level by dragging the slider into the appropriate position.

Figure 60. Navigator view

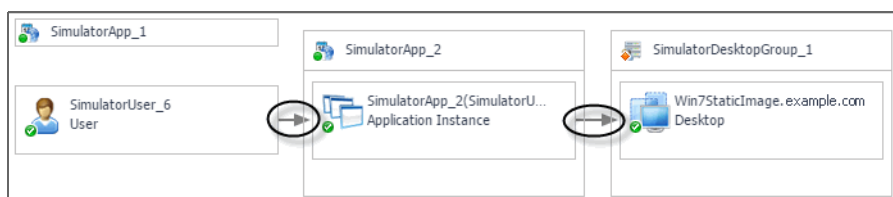


Figure 61. Object health indicators



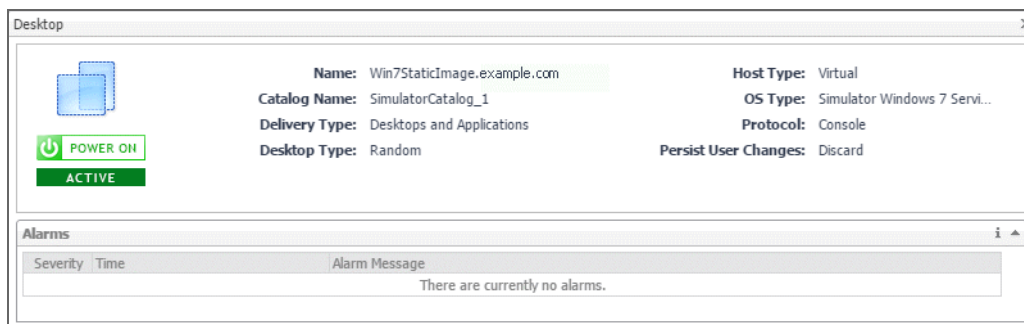
Dependencies between the objects in a map are illustrated with single-directional arrows. The color of the arrow reflects the alarm state of the target object: gray for Normal, yellow for Warning, orange for Critical, and red for the Fatal state.

Figure 62. Object dependencies



To find out more about an object appearing in the dependency map, click the object icon. A dialog box appears, displaying more details about that object. The type and range of information appearing in the dialog box depends on the selected object's type. For example, drilling down on a XenDesktop machine shows the machine name, DNS name, and the type of services hosted on the machine (desktops, applications, or desktops and applications), and the count of user sessions over the selected time range.

Figure 63. Drilling down on XenDesktop machine

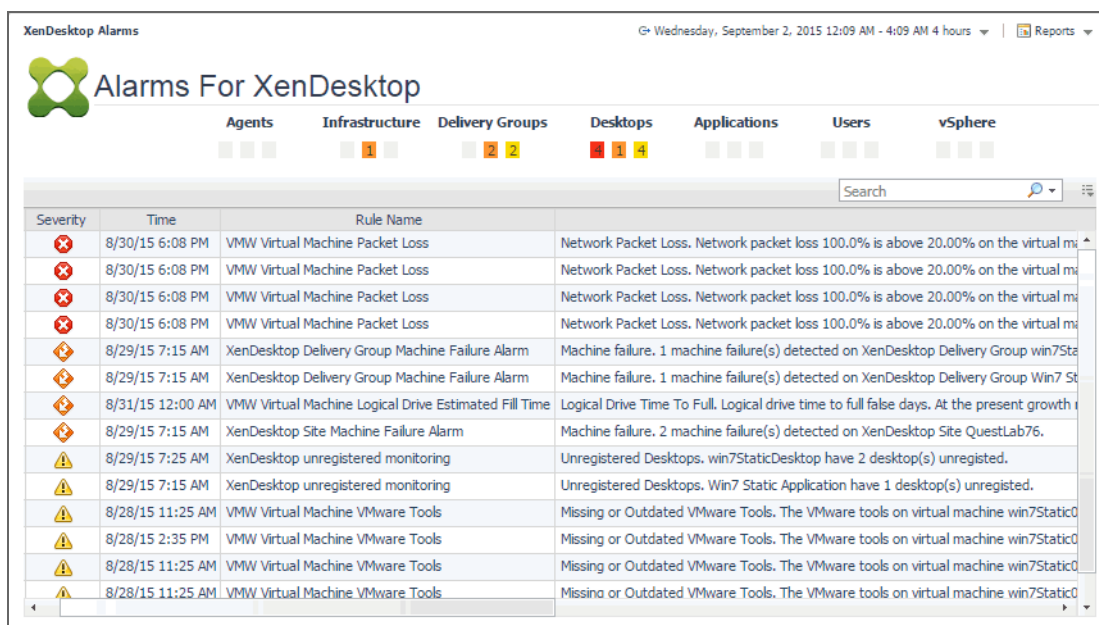


TIP: To return to the XenDesktop Environment dashboard, use the bread crumb trail in the top-left corner.

Exploring XenDesktop Alarms

The XenDesktop Alarms dashboard is a simple dashboard that shows the alarms that have been triggered but not cleared. It can be used to isolate alarms specific to your monitored XenDesktop environment.

Figure 64. XenDesktop Alarms dashboard



Exploring alarm counts

The top part of this dashboard shows the counts of alarms grouped by object type against which the alarms are generated: **Agents**, **Infrastructure**, **Delivery Groups**, **Desktops**, **Applications**, **Users**, and **vSphere**.

Figure 65. Alarms by object type



Each group displays the numbers of alarms in each severity state: Fatal (red), Critical (orange), and Warning (yellow).

Figure 66. Alarms by severity level



When you drill down on an alarm count in an object group, a dialog box displays, showing the list of all alarms generated against the selected object type and severity.

Figure 67. Drilling down on alarm counts

Severity	Time	Rule Name	Alarm Message
Critical (Orange)	8/29/15 7:15 AM	XenDesktop Delivery Group Machine Failure Alarm	Machine failure. 1 machine failure(s) detected on XenDe
Critical (Orange)	8/29/15 7:15 AM	XenDesktop Delivery Group Machine Failure Alarm	Machine failure. 1 machine failure(s) detected on XenDe

Exploring the alarm table

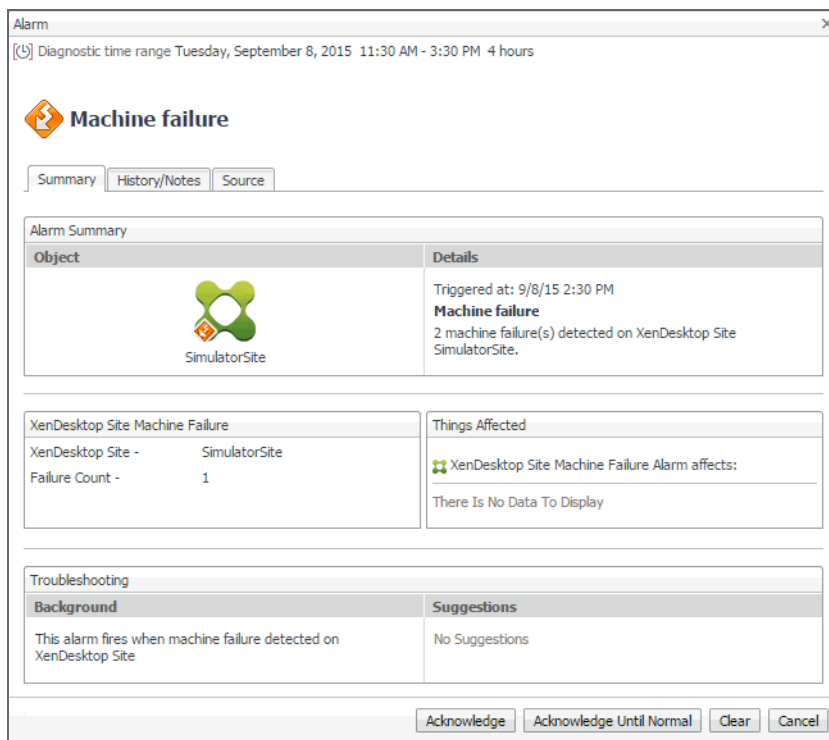
The XenDesktop Alarms dashboard displays a table containing all alarms fired against your monitored objects. For each alarm entry, it displays the associated object type, the alarm severity, when it was generated, the rule name that triggered the alarm, and the alarm message.

Figure 68. Alarm table

Severity	Time	Rule Name	Alarm Message
Critical (Red)	8/30/15 6:08 PM	VMW Virtual Machine Packet Loss	Network Packet Loss. Network packet loss 100.0% is above 20.00% on the virtual machine win7Static008.
Critical (Red)	8/30/15 6:08 PM	VMW Virtual Machine Packet Loss	Network Packet Loss. Network packet loss 100.0% is above 20.00% on the virtual machine win7Static007.
Critical (Red)	8/30/15 6:08 PM	VMW Virtual Machine Packet Loss	Network Packet Loss. Network packet loss 100.0% is above 20.00% on the virtual machine win7Static009.
Critical (Red)	8/30/15 6:08 PM	VMW Virtual Machine Packet Loss	Network Packet Loss. Network packet loss 100.0% is above 20.00% on the virtual machine win7Static010.
Critical (Orange)	8/29/15 7:15 AM	XenDesktop Delivery Group Machine Failure Alarm	Machine failure. 1 machine failure(s) detected on XenDesktop Delivery Group win7StaticDesktop.
Critical (Orange)	8/29/15 7:15 AM	XenDesktop Delivery Group Machine Failure Alarm	Machine failure. 1 machine failure(s) detected on XenDesktop Delivery Group Win7 Static Application.
Critical (Orange)	8/31/15 12:00 AM	VMW Virtual Machine Logical Drive Estimated Fill Time	Logical Drive Time To Full. Logical drive time to full false days. At the present growth rate, logical drive C:\ on
Critical (Orange)	8/29/15 7:15 AM	XenDesktop Site Machine Failure Alarm	Machine failure. 2 machine failure(s) detected on XenDesktop Site QuestLab76.
Warning (Yellow)	8/29/15 7:25 AM	XenDesktop unregistered monitoring	Unregistered Desktops. win7StaticDesktop have 2 desktop(s) unregistered.
Warning (Yellow)	8/29/15 7:15 AM	XenDesktop unregistered monitoring	Unregistered Desktops. Win7 Static Application have 1 desktop(s) unregistered.
Warning (Yellow)	8/28/15 11:25 AM	VMW Virtual Machine VMware Tools	Missing or Outdated VMware Tools. The VMware tools on virtual machine win7Static008 are either out of dat
Warning (Yellow)	8/28/15 2:35 PM	VMW Virtual Machine VMware Tools	Missing or Outdated VMware Tools. The VMware tools on virtual machine win7Static007 are either out of dat
Warning (Yellow)	8/28/15 11:25 AM	VMW Virtual Machine VMware Tools	Missing or Outdated VMware Tools. The VMware tools on virtual machine win7Static009 are either out of dat
Warning (Yellow)	8/28/15 11:25 AM	VMW Virtual Machine VMware Tools	Missing or Outdated VMware Tools. The VMware tools on virtual machine win7Static010 are either out of dat

Clicking any row in the table displays the **Alarm** dialog box, containing additional details about the alarm.

Figure 69. Alarm dialog box

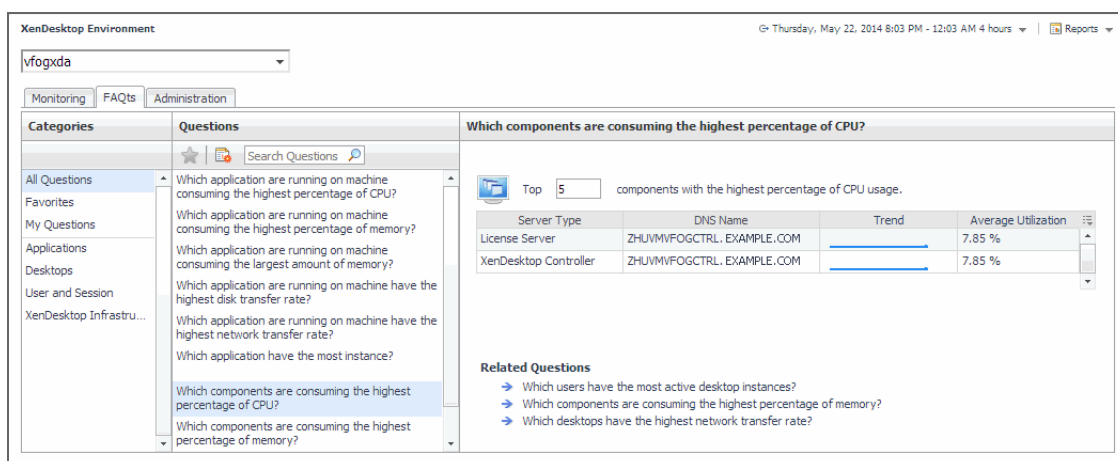


Reviewing Frequently Asked Questions

Foglight™ for Citrix XenDesktop and XenApp offers a collection of frequently asked questions that provide quick insight into resource utilization levels for the applications, desktops, user sessions, and the overall infrastructure in your monitored system. The question mechanism is interactive, guiding you to choose a category and specify additional parameters.

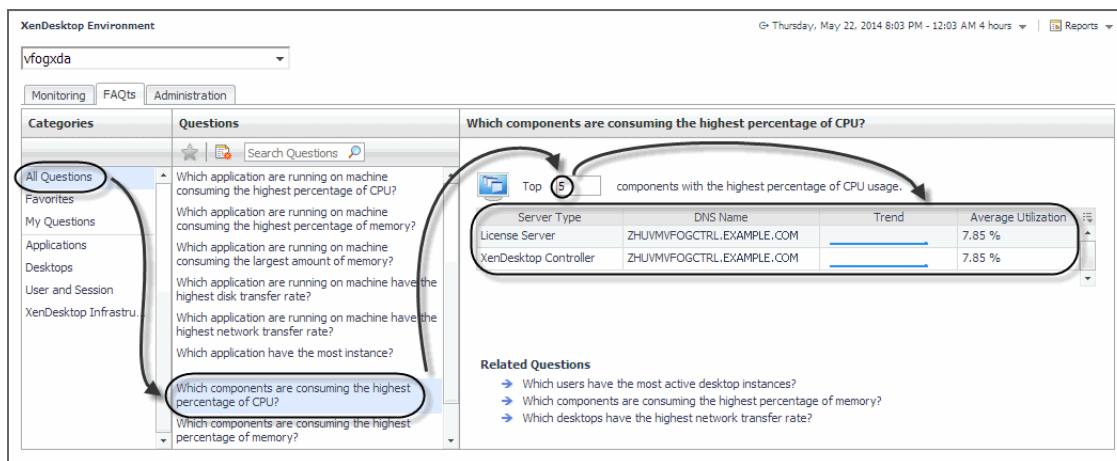
You can find the available questions on the **FAQts** tab of the XenDesktop Environment dashboard.

Figure 70. FAQts tab



On this tab, the **Categories** pane several question groups. Selecting a category shows the questions belonging to that category in the **Questions** pane. From there, clicking a question shows the answer on the right.

Figure 71. Choosing questions and reviewing answers

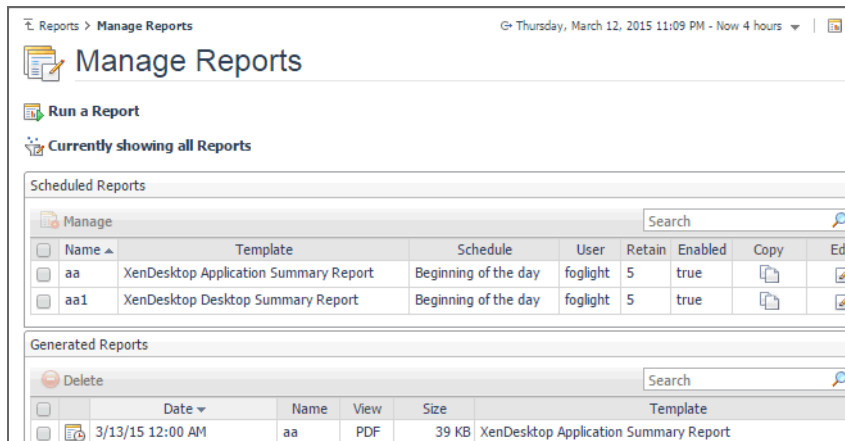


Generating reports

Foglight™ for Citrix XenDesktop and XenApp includes a report generation ability. This allows you to create reports using a set of predefined templates to report on the various aspects of your virtual environment. Foglight for Citrix XenDesktop and XenApp includes a collection of predefined report templates.

You can generate, copy, and edit reports using the Manage Reports dashboard included with the Management Server.

Figure 72. Manage Reports dashboard



For complete information about this dashboard, see the *Foglight User Help*.

The following templates are available with Foglight for Citrix XenDesktop and XenApp.

Table 26. Report templates

Report Template	Use it to...
XenDesktop Application Summary	Find out which applications have the most instances, and to identify the ones with the slowest application sessions, highest CPU and memory utilization, and highest I/O transfer rates.

Table 26. Report templates

Report Template	Use it to...
XenDesktop Desktop Summary	Find out which desktops have the most sessions, and to identify the ones with the slowest sessions, highest CPU and memory utilization, and highest I/O transfer rates.
XenDesktopSite Summary	Review general information about the monitored XenDesktop site along with performance trends in session counts, logon duration, machine and connection failures. This report also provides general information about the existing delivery groups along with performance trends in their session counts, connected users, machine and connection failures.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit <https://www.quest.com/>.

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.