

Foglight® for VMware Horizon View 6.1.0  
**User and Reference Guide**



© 2022 Quest Software Inc.

## ALL RIGHTS RESERVED.

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

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

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

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

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

## Patents

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

## Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. "Apache HTTP Server", Apache, "Apache Tomcat" and "Tomcat" are trademarks of the Apache Software Foundation. Google is a registered trademark of Google Inc. Android, Chrome, Google Play, and Nexus are trademarks of Google Inc. Red Hat, JBoss, the JBoss logo, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries. CentOS is a trademark of Red Hat, Inc. in the U.S. and other countries. Fedora and the Infinity design logo are trademarks of Red Hat, Inc. Microsoft, .NET, Active Directory, Internet Explorer, Hyper-V, Office 365, SharePoint, Silverlight, SQL Server, Visual Basic, Windows, Windows Vista and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. AIX, IBM, PowerPC, PowerVM, and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Java, Oracle, Oracle Solaris, PeopleSoft, Siebel, Sun, WebLogic, and ZFS are trademarks or registered trademarks of Oracle and/or its affiliates in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries. Products bearing the SPARC trademarks are based on an architecture developed by Oracle Corporation. OpenLDAP is a registered trademark of the OpenLDAP Foundation. HP is a registered trademark that belongs to Hewlett-Packard Development Company, L.P. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries. Novell and eDirectory are registered trademarks of Novell, Inc., in the United States and other countries. VMware, ESX, ESXi, vSphere, vCenter, vMotion, and vCloud Director are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Sybase is a registered trademark of Sybase, Inc. The X Window System and UNIX are registered trademarks of The Open Group. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. "Eclipse", "Eclipse Foundation Member", "EclipseCon", "Eclipse Summit", "Built on Eclipse", "Eclipse Ready", "Eclipse Incubation", and "Eclipse Proposals" are trademarks of Eclipse Foundation, Inc. IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Apple, iPad, iPhone, Mac OS, Safari, Swift, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Ubuntu is a registered trademark of Canonical Ltd. Symantec and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. OpenSUSE, SUSE, and YAST are registered trademarks of SUSE LLC in the United States and other countries. Citrix, AppFlow, NetScaler, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. AlertSite and DéjàClick are either trademarks or registered trademarks of Boca Internet Technologies, Inc. Samsung, Galaxy S, and Galaxy Note are registered trademarks of Samsung Electronics America, Inc. and/or its related entities. MOTOROLA is a registered 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.

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

Foglight for VMware Horizon View User and Reference Guide  
Updated - April 2022  
Foglight Version - 6.1.0  
Cartridge Version - 6.1.0

# Contents

<b>Manage desktops in virtual environments</b>	<b>6</b>
Foglight for VMware Horizon View overview	6
Foglight for VMware Horizon View elements	6
Navigation basics	7
Foglight browser interface elements	7
Breadcrumbs	8
Time range	9
Sortable lists	9
Alarms and status indicators	10
Mouse-over actions	10
<b>Interact with Foglight for VMware Horizon View dashboards</b>	<b>11</b>
Interact with Foglight for VMware Horizon View	11
Prepare your VMware Horizon View environment for monitoring	12
Domain user and Key Distribution Center	12
Agent Manager configuration	13
Connection server PowerShell configuration	14
Host configuration (WinRM)	15
Host configuration (DCOM)	16
Troubleshoot agent collection problems	19
Explore administrative tasks	21
Tasks area	21
Agents view	22
Manually add View instances	23
Discover View instances	27
Add Host Agents	32
Managing certificates	35
Use the VMware View Environment dashboard	39
Details tab	40
Administration tab	40
Navigating between View server instances	40
Explore the VMware View Environment Details tab	40
Work with tiles	41
Use the Quick View	43
Explore user sessions	43
Explore desktops	44
Explore Horizon Pools	45
Use the VMware Explorer	46
Virtual Infrastructure view	47
VMware Explorer View	48
Accessing VMware® actions and tasks	52
<b>Reference</b>	<b>54</b>
Views	54

Action panel	55
Administration tab	55
Agents view	58
Alarms List view	58
Cost tab	59
CPU tab	60
Event Analytics tab	61
FAQts view	63
Memory tab	64
Monitor tab	65
Performance tab	67
Processes tab	69
Quick View	70
Related Objects views	71
Resource Pools Relationship Tree view	71
Shares tab	72
Storage tab	74
Summary tab	75
Utilizations views	76
Virtual Environment Overview	78
Virtual Infrastructure view	79
VMware Explorer Primary view	81
VMs tab	83
<b>About Us</b>	<b>85</b>
We are more than just a name	85
Our brand, our vision. Together.	85
Contacting Quest	85
Technical support resources	85

# Manage desktops in virtual environments

This guide provides information on how to investigate the performance of your desktop virtualization environment using Foglight® for VMware Horizon View. Read this guide straight through in an effort to acquire an overall understanding of the workings and capabilities of Foglight for VMware Horizon View, or use it as a reference whenever you require specific information about this product.

This section introduces you to Foglight for VMware Horizon View and provides essential foundational information:

- [Foglight for VMware Horizon View overview](#)
- [Navigation basics](#)

## Foglight for VMware Horizon View overview

Foglight for VMware Horizon View monitors a virtual desktop environment, providing performance metrics, alarms, and alerts to help you better manage your environment, from user desktops to related infrastructure.

Foglight for VMware Horizon View gathers extensive performance metrics and presents that data in a graphical interface, utilizing architectural diagrams, graphs, and drilldown screens to quickly identify virtual desktop problems. This allows users to browse through their virtual infrastructure to identify desktop performance, connection, and infrastructure issues.

It fully supports VMware®, vCenter®, and vSphere® environments.

## Foglight for VMware Horizon View elements

Foglight for VMware Horizon View provides monitoring capabilities so that all elements of a virtual desktop environment are considered. A typical VMware View environment contains one or more user sessions and related infrastructures:

- **View Infrastructure.** The VMware View infrastructure is composed of one or more connection servers, transfer servers, and security servers.
- **User Session.** Shows the connected users, their session details, and the session type (for example, VDI user session, Terminal Server, or physical desktop). Each user has one or more sessions.
- **vSphere Objects.** This underlying infrastructure is broken down by cluster, datastore, ESX® hosts, and resource pools.
- **Desktops.** Shows the resource utilization values for a selected VM, Terminal Server Host, or Physical Host.
- **Horizon Pools.** Shows the health of pools in the View Instance.

You can view the overall state of all these components on the VMware View Environment dashboard. For more information on this dashboard, see [Use the VMware View Environment dashboard](#).

# Navigation basics

This section describes the basic Foglight for Hyper-V navigation techniques necessary for using Foglight for VMware Horizon View:

- [Foglight browser interface elements](#)
- [Breadcrumbs](#)
- [Time range](#)
- [Sortable lists](#)
- [Alarms and status indicators](#)
- [Mouse-over actions](#)

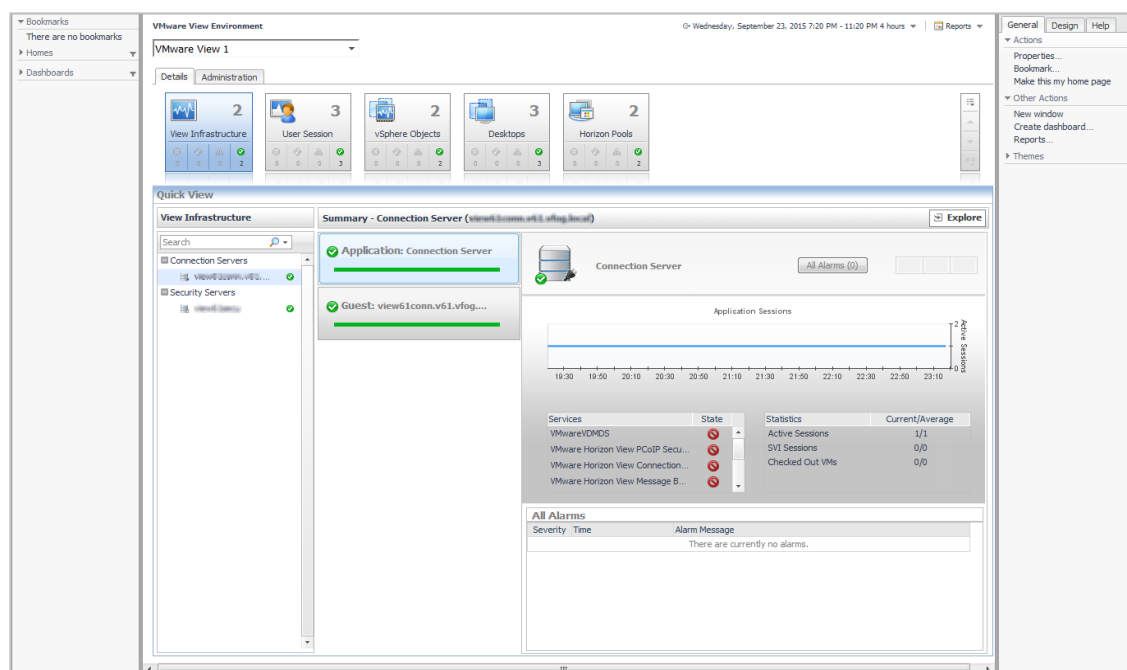
For more information about Foglight for Hyper-V navigation, see the *Foglight User Guide* and *Foglight Administration and Configuration Guide*.

## Foglight browser interface elements

Depending on your user roles, you may see either the contents of the first bookmark (the Welcome page is the default) listed under Bookmarks, or a home page. For further details about roles, see the *Foglight User Guide*.

Typically, the browser interface is divided into three panels: the navigation panel on the left, the display area in the middle, and the action panel on the right.

**Figure 1. Foglight browser interface elements**



## Navigation panel

The navigation panel operates like a drawer. Its default state is open. To close the navigation panel, click the arrow at the far left of the Foglight for Hyper-V browser interface. Click that arrow again to open the navigation panel.

The navigation panel lists all of the dashboards that are available to the current user for viewing. You can use the navigation panel to select a dashboard to view in the display area. To access a specific dashboard, open the appropriate module (VMware View, for example).

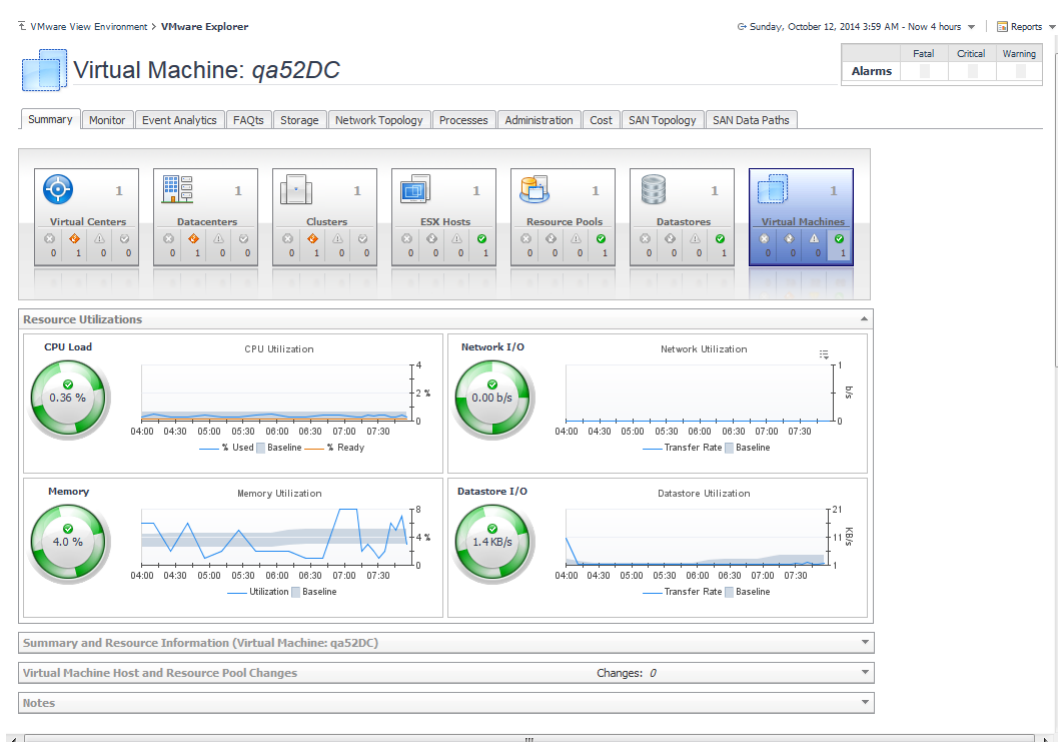
The navigation panel also provides access to the Foglight for Hyper-V Administration and Configuration areas.

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

## Display area

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

Figure 2. Display area



## Action panel

The action panel operates like a drawer. Its default state is closed. To open the action panel, click the arrow at the far right of the Foglight for Hyper-V browser interface. Click that arrow again to close the action panel.

The action panel contains the various actions and tasks you can perform with the current dashboard. It also contains views and data that you can add to a dashboard or report you are creating and provides access to the online help files.

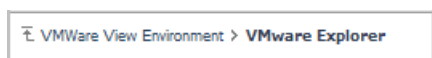
## Breadcrumbs

If you drill down into various levels across dashboards, a trail of breadcrumbs is left at the top of the current dashboard. This trail provides you with context. It also provides you with the name of the level you are currently viewing and with a simple mechanism for returning to any of its related parent levels.



The following breadcrumb trail was created while drilling down from the VMware View Environment dashboard into the VMware Explorer dashboard. Each item within a breadcrumb trail is a hyper link to a previously viewed parent level.

**Figure 3. Breadcrumbs**



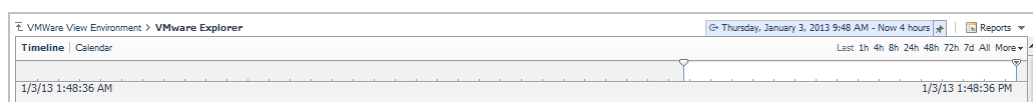
For more information about using VMware View dashboards, see [Interact with Foglight for VMware Horizon View dashboards](#).

## Time range

The default behavior of Foglight for Hyper-V is to display metrics, alerts, and messages that have occurred within the last four hours. This time range, however, is configurable.

To configure the Time Range, use the Time Range popup, which you can access from the upper right corner of the Foglight for Hyper-V browser interface.

**Figure 4. Time range**



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

For more information about modifying the time range, see the *Foglight for Hyper-V User Guide*.

## Sortable lists

In certain Foglight for VMware Horizon View dashboards, some levels of views contain sortable lists. An example of this is the VMware Explorer dashboard Virtual Machine table displayed below.

**Figure 5. Sortable lists**

Virtual Machines at PE R610s					
Search					
Virtual Machine	Status	CPU	Memory	Host	Status
Name				Name	
MoveMe-01	✓	n/a	n/a	10.4.45.110	✓
OM07-QMX	✓	n/a	n/a	10.4.45.110	✓
PS_SnapshotTest_STLVC	✓	n/a	n/a	10.4.45.116	⚠

It is possible to sort this list by column using any of the column headings. Click a column heading once to sort the list in ascending order. The list is redrawn according to your specification. Click the column heading again to re-sort the list in descending order.

This is handy when you want to have an organized view of virtual machines or host objects sorted by name, status, or some other criterion.

# Alarms and status indicators

Foglight for VMware Horizon View uses status indicators to show the alarm states of the objects within the virtual infrastructure. Four status indicators (fatal, critical, warning, and normal), are used throughout the Foglight for VMware Horizon View dashboards. An alarm table, located at the top of the VMware Explorer views, highlights the key alarms as shown in the following illustration.

Figure 6. Alarms and status indicators

	Fatal	Critical	Warning
Alarms	2	6	24

## Mouse-over actions

Many items within the Foglight for VMware Horizon View dashboards display additional information when you hover the cursor over them. For example, when you hover the cursor over a graph you are likely to see a specific value or values that correspond) to the position of the cursor. When you hover the cursor over an individual metric, you are likely to see a small descriptive popup.

# Interact with Foglight for VMware Horizon View dashboards

After installing Foglight for VMware Horizon View, you can monitor the components of your virtual desktop environment. These components include user sessions, the VMware View infrastructure, and the supporting vSphere® infrastructure.

For more information, see these topics:

- [Interact with Foglight for VMware Horizon View](#)
- [Prepare your VMware Horizon View environment for monitoring](#)
- [Explore administrative tasks](#)
- [Use the VMware View Environment dashboard](#)
- [Explore the VMware View Environment Details tab](#)
- [Use the VMware Explorer](#)
- [Accessing VMware® actions and tasks](#)

## Interact with Foglight for VMware Horizon View

When you install Foglight for VMware Horizon View, a set of predefined dashboards enables you to view the performance of your virtual system at a glance. They allow you to ensure consistent application performance by drilling down for details from higher-level components such as clusters, hosts, and virtual machines, to viewing detailed specifics about each component, such as CPU utilization and network I/O.

Foglight for VMware Horizon View relies on the VMware Horizon View agents to collect data from monitored hosts, using a desired collection method. Prior to creating VMware Horizon View agents, it is critical to configure the servers to be monitored. There are a few settings that must be made before the agents can successfully collect data. For more information, see [Prepare your VMware Horizon View environment for monitoring](#).

The **Administration** tab of the VMware View Environment dashboard lists the available View Connection Server agents and shows their status, and provides the ability to create agents and modify their properties. For more information, see [Explore administrative tasks](#) and [Manually add View instances](#).

Next, familiarize yourself with the VMware View Environment dashboard. This is the dashboard that you see when you click **Dashboards > VMware View**. For more information about this dashboard and the associated views, see [Use the VMware View Environment dashboard](#).

To see in-depth details about a monitored server, cluster, or virtual machine, use the VMware Explorer dashboard. You can drill down to this dashboard from the **Details** tab. For further information, see [Use the VMware Explorer](#).

To read about additional features, such as planning for virtual machine migrations or reviewing topology object instances and expired data, see [Accessing VMware® actions and tasks](#).

# Prepare your VMware Horizon View environment for monitoring

Prior to creating VMware Horizon View agents, it is critical to configure the servers to be monitored. There are a few settings that must be made before the agents can successfully collect data. These steps should be done on each relevant host prior to running the **Discover View Instances** wizard or manually creating VMware Horizon View agents.

When using the **Discover View Instances** wizard to create VMware Horizon View monitoring agents, several agents are created:

- A Connection Server agent is created to monitor the Connection Server.
- A Host agent is created for each Connection, Security, and Transfer Server.
- A Host agent is created for each physical machine (if any) available in your VMware Horizon View environment for checkout.

**To prepare the VMware Horizon View environment for monitoring, execute the following tasks:**

- 1 Domain task. Determine a domain user, Key Distribution Center, and event database password required for agent configuration. For more information, see [Domain user and Key Distribution Center](#).
- 2 Agent Manager tasks. Verify whether the Agent Manager host is configured correctly. For more information, see [Agent Manager configuration](#).
- 3 Connection Server tasks. Configure PowerShell execution policy. For more information, see [Connection server PowerShell configuration](#).
- 4 Monitored Hosts tasks. Choose to monitor the environment using either WinRM (recommended) or DCOM, and configure the monitored hosts accordingly. These tasks apply to all Connection, Security, and Transfer Servers, as well as any physical hosts available for checkout. For more information, see [Host configuration \(WinRM\)](#) and [Host configuration \(DCOM\)](#).

For a list of problems that you might encounter while monitoring your environment using Foglight for VMware Horizon View, and solutions available to troubleshoot these problems, see [Troubleshoot agent collection problems](#).

## Domain user and Key Distribution Center

To correctly configure the view agent, the following information must be identified:

- **The domain user account to be used for monitoring.** This user does not need any special domain privileges, but must be in the local administrators group of each Connection Server to be monitored.  
  
The domain user also needs to be granted the *Administrator (Read-only)* role in the “View Administrator” console, which allows the view agent to collect information from the View environment. To grant this role to a domain user:
  - a Create a domain user in Active Directory®.
  - b Open the “View Administrator” console, navigate to *View Configuration*, and click **Administrators**.
  - c Click **Add User or Group** and add the newly created domain user.
  - d Select *Administrators (Read only)* role to this domain user.
  - e Remote connect to the Connection Server. Using the Server Manager, click **Configuration > Local Users and Groups > Groups > Administrators**, and right click to open the *Administrators Properties* dialog box. Add the newly created domain user to the *Administrators* group.
- **The Key Distribution Center (KDC).** If choosing to monitor the environment using WinRM (recommended), the Kerberos authentication is used. Kerberos is enabled by default in all Windows® domains, and all domain controllers act as KDCs. It is usually sufficient to specify just the domain in the

agent settings, *MyDomain.local*, instead of the fully qualified domain name (FQDN) of a domain controller, *MyDC.MyDomain.local*. However, to ensure that the agent uses a specific domain controller as the KDC, use its FQDN.

**i** | **NOTE:** For more information about KDC, see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa378170%28v=vs.85%29.aspx>.

- **The Event Database password.** The VMware Horizon View agent monitors the View Event Database. You must know the password for the Event Database to completely configure the VMware Horizon View agent. To confirm this password, go to **View Configuration > Event Configuration** in the VMware View Administrator instance.

The Event Database password is optional. The event database configuration, including the access password, is defined by the Event Database administrator during the event database installation and setup. For more information about this topic, refer to the VMware® documentation. The password should be the same as the password configured in the VMware View Administration, **View Configuration > Event Configuration** option.

**i** | **NOTE:** When the password is specified in the view agent properties, it enables the event-based rules in the cartridge. When no password is specified, the alarms from the event database are not logged.

## Agent Manager configuration

Before configuring a collection method, you must ensure that the Agent Manager machine on which the View Connection Server Agent resides can connect to the View Connection Server. Follow the configuration checks in this section to verify the connection.

### Step 1: Verify the registry key

If running Agent Manager on a Windows® host and using WinRM (recommended), verify that the Kerberos is properly configured. Verify whether the following registry key exists and add it, if it does not exist.

**Path:** HKEY\_LOCAL\_MACHINE/SYSTEM/CurrentControlSet/Control/Lsa/Kerberos/Parameters

**Value Name:** allowTGTSessionKey

**Value Type:** REG\_DWORD

**Value:** 1

### Step 2: Verify the name resolution

Name resolution must work from the Agent Manager host to the View Connection Server.

**To verify that the name resolution resolves:**

- 1 Open a command prompt and verify that you can ping the View Connection Server using its fully-qualified domain name.
- 2 If this fails to resolve, contact your domain administrator or manually edit the hosts file on the Agent Manager host.

### Step3: Verify the access port

The Agent Manager must be configured to access port **389** of the target Connection Server if not using SSL.

The Agent Manager must be configured to access port 636 of the target Connection Server if using SSL.

# Connection server PowerShell configuration

The View Connection Server Agent must be able to execute PowerShell commands on the monitored Connection Servers.

## Step 1: Set ExecutionPolicy

### **To set the execution policy:**

- 1 Log in to the View Connection Server machine using an account with Administrator privileges.
- 2 Open a command prompt and type: `powershell.exe`
- 3 At the PowerShell prompt, type: `Get-ExecutionPolicy`
- 4 The message *Unrestricted* appears.  
If this message does not appear, type: `Set-ExecutionPolicy Unrestricted`
- 5 When prompted, type `y`  
The View Connection Server now has unrestricted access to run PowerShell commands.

## Step 2: Verify the user account has sufficient privileges to run VMware Horizon View cmdlets

The View Connection Server Agent must have a user account with the correct credentials to run VMware Horizon View cmdlets on the Connection Server.

### **To verify the user account privileges:**

- 1 Log into the View Connection Server using the same credentials as the View Connection Server Agent.
- 2 Open a command prompt and type: `powershell.exe`
- 3 Load the VMware Horizon View snapins. Type the following cmdlet:  

```
C:\Program Files\VMware\VMware View\Server\extras\PowerShell\add-snapin.ps1
```

The `Snapin.PS1` script adds the VMware Horizon View snapins. These snapins consist of all the cmdlets that are typically used in a VMware Horizon View environment.
- 4 Verify that the View Connection Server Agent can run the necessary VMware Horizon View cmdlets. To test, this, type one or more of the following cmdlets:  

```
Get-ViewVC  
Get-ConnectionBroker  
Get-Monitor  
Get-RemoteSession
```

Values specific to the issued cmdlet should be returned.

## Step 3: Additional configuration

In addition to this Powershell configuration, the Connection Server must also be configured for either WinRM or DCOM as described in [Host configuration \(WinRM\)](#) and [Host configuration \(DCOM\)](#).

# Host configuration (WinRM)

When using this collection method to obtain information from remote hosts, Foglight for VMware Horizon View relies on WinRM to expose the data.

- IMPORTANT:** If you plan a user number higher than 140 in your VDI environment, you must increase the maximum envelope size for the connection server. For more information, see [Data returned by PowerShell may exceed the default envelope size of WinRM when the scale of VMware Horizon View is large enough.](#)

## Step 1: Configure WinRM

This section includes some specific information related to configuring WinRM to remotely access the monitored hosts. It should not be used as a complete reference for this Windows® component.

For complete information about configuring the WinRM service, refer to the WinRM documentation. To quickly access the WinRM help, type `WinRM` at the command prompt.

- NOTE:** If an Access is denied error occurs when running WinRM commands, run the command-line tool as an administrator or temporarily disable the User Account Control (UAC). For instructions on disabling the UAC, see: [http://technet.microsoft.com/en-us/library/cc709691\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx).

When the WinRM configuration is complete, ensure that the Windows® Remote Management service is started:

- Check the existing configuration.** Open a command prompt as administrator. Type:

```
winrm quickconfig
```

The message appears, specifying whether the WinRM is already configured. If it is not, you are prompted to enable WinRM and open the required ports in the firewall.

- Create a listener. Type:

```
winrm create winrm/config/listener?Address=*&Transport=HTTP
```

This command creates a listener if one does not already exist. If one exists, a message appears.

- Enable Kerberos authentication.** Type:

```
winrm set winrm/config/service/auth @{Kerberos="true"}
```

Choose either to allow non-encrypted (HTTP) communication or to require encryption (HTTPS). This choice corresponds to the *Use SSL (True/False)* section during agent configuration. When choosing to require encryption, you must have your certificate thumbprint. See your domain administrator for details.

### To allow non-encrypted communication:

- Type: `winrm set winrm/config/service @{AllowUnencrypted="true"}`

### To require encrypted communication:

- Type: `winrm create winrm/config/listener?Address=*&Transport=HTTPS  
@{CertificateThumbprint="PASTE_CERTIFICATE_THUMBPRINT_HERE"}`

- NOTE:** This type of authentication requires that WinRM be configured with an HTTPS listener and that an appropriate certificate exists to identify the machine on which WinRM is running. In addition to this WinRM configuration, the server that is running the Agent Manager must be configured to trust the WinRM Server's Certificate. You must configure the Agent Manager on a remote host to trust third-party certificates.

## Step 2: Verify the WS-Man communication port

The port returned by the command below is used in the *WS-Man Communication Port* field during agent configuration. The *WS-Man Communication Port* is set to 5985 by default. Most Windows® versions use 5985/5986; however, some versions are known to use other port values, such as 80/443.

### **To verify the WS-Man communication port:**

- From a command prompt, type: `winrm enumerate winrm/config/listener`

## Host configuration (DCOM)

When using this collection method to collect process information from remote hosts, Foglight for VMware Horizon View relies on DCOM to access the Windows® Management Instrumentation (WMI) infrastructure on the remote hosts, to connect to virtual and physical machine hosts and collect their metrics.

The following information must be taken into consideration when using this collection method with Foglight for VMware Horizon View:

- Only a domain user that is in the monitored hosts administrators group is allowed to collect data.
- Using the DCOM with Foglight for VMware Horizon View to collect metrics through a firewall requires additional configuration steps. For more information, see [Configure firewall settings manually](#).
- This collection method may require that the Remote Registry service be running on the target host. Some versions of Microsoft® Windows have this service disabled by default. It is recommended that you verify whether this service is running and is configured to start automatically.
  - NOTE:** If the Remote Registry service starts after attempting collection, restart the Foglight Agent Manager for the collection to be successful.
- Some restrictions on the Windows Server® limit the access to certain areas of the registry that prohibit the Connection Server Agent from collecting data. For more information, see [Enable DCOM on a Windows Server](#). Alternatively, use WinRM to collect process data from these hosts.

## Configure firewall settings manually

When using DCOM to collect metrics through a firewall, configure the firewall manually, then create and run a configuration script (as shown in [Configure firewall settings using a script](#)).

### **To configure firewall settings manually:**

- 1 Enable all incoming traffic to the default DLL surrogate (`dllhost.exe`).
  - a Create a rule that allows all incoming traffic for the file: `%systemroot%\system32\dllhost.exe`
  - b **64-bit systems only.** Create a rule that allows all incoming traffic for the file: `%systemroot%\SysWOW64\dllhost.exe`
- 2 Enable the COM+ Network Access (DCOM-In) rule for the active profile.
- 3 Enable all rules in the File and Printer sharing group for the active profile.

**NOTE:** The scope defined for the updated rules should include the host on which the Management Server is running.

## Enable DCOM on a Windows Server

Use the following process to bypass the access restrictions that prohibit the View Connection Server Agent from collecting data from a monitored system.

### **To collect data from Windows® using DCOM:**

- 1 Log in to the target remote host as the Administrator.
- 2 Start the Windows Registry Editor (`regedit.exe`).
  - TIP:** It is recommended that you create a backup copy of the Windows Registry before making any changes, so that you can revert the changes, if necessary.



- 3 If you are prompted to allow the Regedit program to make changes to the computer, click **Yes**.
- 4 For each of the following registry keys:
  - HKEY\_CLASSES\_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
  - HKEY\_CLASSES\_ROOT\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
  - HKEY\_CLASSES\_ROOT\Wow6432Node\CLSID\{72C24DD5-D70A-438B-8A42-98424B88AFB8}
  - a Right-click the key, and from the shortcut menu that appears, select **Permissions**.
  - b In the Permissions dialog box, click **Advanced**.
  - c In the Advanced Security Settings dialog box that appears, open the **Owner** tab.
  - d In the Change Owner to list, select the account with which you are currently logged in.
  - e Click **OK** to close the Advanced Security Settings dialog box.
  - f In the Permissions dialog box, click **OK** to close it.
  - g In the Registry Editor window, right-click the same registry key again and, from the shortcut menu that appears, select **Permissions**.
  - h In the Permissions dialog box that appears, select the **Administrators** group.
  - i Grant the Full Control permissions to this group by selecting the **Allow** check box.
  - j In the Permissions dialog box, click **OK** to close it.
  - k Close the Windows Registry Editor.
- 5 Continue with [Configure firewall settings using a script](#).

## Configure firewall settings using a script

### *To configure firewall settings using a script:*

- 1 On the target machine create the file *firewall-config.ps1* containing the following script.
 

```
*
*
* QUEST PROPRIETARY INFORMATION
*
* This software is confidential. Quest Software Inc., or one of its
* supplied this software to you under the terms of a license agreement,
* nondisclosure agreement or both. You may not copy, disclose, or use this
* software except in accordance with those terms.
*
* Copyright 2017 Quest Software Inc.
* ALL RIGHTS RESERVED.
*
* QUEST SOFTWARE INC. MAKES NO REPRESENTATIONS OR WARRANTIES
* ABOUT THE SUITABILITY OF THE SOFTWARE, EITHER EXPRESS
* OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED
* WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
* PARTICULAR PURPOSE, OR NON-INFRINGEMENT. QUEST SHALL
* NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE
```

```

* AS A RESULT OF USING, MODIFYING OR DISTRIBUTING
* THIS SOFTWARE OR ITS DERIVATIVES.
*
$OS = Get-WmiObject Win32_OperatingSystem
$OSBuildNumber = $OS.BuildNumber
$OSCaption = $OS.Caption
$useAdvancedFirewall = $true
$COMNetworkAccessGroup = "COM+ Network Access (DCOM-In)"
if (($OSBuildNumber -eq 2600) -or ($OSBuildNumber -eq 3790)) {
    $useAdvancedFirewall = $false
}
if ($OSBuildNumber -eq 7600) {
    # Windows® 7
    $COMNetworkAccessGroup = "Windows Management Instrumentation (WMI)" }
if ($useAdvancedFirewall) {
    Echo "Configuring firewall for Windows"
    netsh advfirewall firewall add rule name="DLL Host (32-Bits)"
    dir=in action=allow program="%systemroot%\system32\dllhost.exe"
    netsh advfirewall firewall add rule name="DLL Host (64-Bits)"
    dir=in action=allow program="%systemroot%\SysWOW64\dllhost.exe"
    netsh advfirewall firewall set rule
    group=$COMNetworkAccessGroup new enable=yes
    netsh advfirewall firewall set rule group="File and Printer
    Sharing" new enable=yes
}
else {
    Echo "Configuring firewall for Windows XP/2003"
    netsh firewall add allowedprogram
    "%systemroot%\system32\dllhost.exe" "DLL Host (32-Bits)" ENABLE
    netsh firewall add allowedprogram
    "%systemroot%\SysWOW64\dllhost.exe" "DLL Host (64-Bits)" ENABLE
    netsh firewall add portopening TCP 135 "DCE/RPC Locator
    service" ENABLE
    netsh firewall set service FileAndPrint ENABLE}

```

## 2 Run the script with the Administrator's privileges by issuing the following command:

```
powershell -File firewall-config.ps1
```

# Troubleshoot agent collection problems

This section provides information about problems that you might encounter while monitoring your environment using Foglight for VMware Horizon View, and describes the solutions available to troubleshoot these problems.

## Data returned by PowerShell may exceed the default envelope size of WinRM when the scale of VMware Horizon View is large enough

### Summary

Data collected by the VMware Horizon View agent by PowerShell command-lets through WinRM may exceed the default envelope size of WinRM when the scale of VMware Horizon View is large enough.

The maximum envelope size for the connection server and for the VMware Horizon View agent may be different. For the connection server, the default value of `MaxEnvelopeSizekb` is 150. For the Client (VMware Horizon View agent), the default value of `MaxEnvelopeSizekb` is 15,360,000 (about 15,000 \* 1024, which is 100 times bigger than the default value on Server side).

### Solution

- 1 Run the following command on the connection server, to enlarge the default value:

```
winrm set winrm/config '@{MaxEnvelopeSizekb="NEW_LARGER_VALUE"}'
```

If `NEW_LARGER_VALUE` is less than 15,000, the problem is resolved. Otherwise, continue with [Step 2](#).

- 2 On the Agent Manager side, enlarge the envelope size by inserting the following JVM parameter:

```
vmparameter.1 = "-Drdsl.winrm.maxenvelopesizekb=NEW_LARGER_VALUE_2";
```

**NOTE:** The value of `NEW_LARGER_VALUE_2` should equal to `1024*NEW_LARGER_VALUE`.

in the following file:

<`FGL_INSTALL_PATH`>\state\default\config\baseline.jvmargs.config (for Foglight for Virtualization, Enterprise Edition 7.0 or later)

or

<`FGL_INSTALL_PATH`>\state\default\config\vm.config (for Foglight for Virtualization, Enterprise Edition versions prior to 7.0)

## Configure LDAP over SSL for Active Directory LDS

### Summary

By default, SSL is not enabled for Active Directory® Lightweight Directory Services (AD LDS), previously named Active Directory Application Mode (ADAM). VMware Horizon View monitoring fails in this case.

### Solution

#### To use LDAP over SSL for Active Directory LDS:

- 1 Obtain a server authentication certificate from a trusted certification authority (CA).
  - The CA can be a trusted CA in your organization or a trusted third-party CA.
  - The certificate should issue to the **FQDN of the server name**.
  - The certificate should contain the **Server Authentication purpose**.
  - The certificate should contain the **Private Key**.

For more information about installing and using a CA, see Certificate Services on <http://go.microsoft.com/fwlink/?LinkID=48952>.

2 Install a server authentication certificate.

- If the certificate is shared with other services on the server, install the certificate to the **computer's personal store**.
- If the certificate is used for AD LDS only, install the certificate to the **AD LDS instance's personal store**.

**i NOTE:** The VMware Horizon View AD LDS instance name is VMwareVDMDS. Ensure that you install the certificate to that service account's personal store if you are configuring for VMware Horizon View.

For more information about installing a certificate, see section "Step 1: Install a server authentication certificate" of the "Configuring LDAP over SSL Requirements for AD LDS" topic on [http://technet.microsoft.com/en-us/library/cc725767\(v=ws.10\).aspx#BKMK\\_1](http://technet.microsoft.com/en-us/library/cc725767(v=ws.10).aspx#BKMK_1).

3 Configure permissions on the server authentication certificate.

In order to use the certificate for authentication, the service account running the AD LDS should have **Read** access of the private key. By default, the service account is **NETWORK SERVICE**. If you use another account to run the service, you must grant the permission to that account.

**If the certificate is installed in the computer's personal store:**

- a Click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.
- b Type **mmc** to open Microsoft® Management Console (MMC).
- c Click **File**, click **Add/Remove Snap-in**, select the **Certificates** snap-in in Available snap-ins, and then click **Add**.
- d In **Add or Remove Snap-ins**, select **Computer account** to view the certificates, and then click **Next**.
- e In **Add or Remove Snap-ins**, select **Local computer**, and then click **Finish**.
- f In **Add or Remove Snap-ins**, click **OK**.
- g In the console tree, expand **Certificates(Local Computer)**, expand **Personal**, and then expand **Certificates**.
- h Right click a certificate, select **All Tasks**, and then click **Manage Private Keys**.
- i Add the permission to the service account. Ensure that it has **Read** permission of the private key.

**If the certificate is install in the AD LDS instance's personal store:**

- Follow the instructions in section "Step 2: Configure permissions on the server authentication certificate" of the "Configuring LDAP over SSL Requirements for AD LDS" topic on [http://technet.microsoft.com/en-us/library/cc725767\(v=ws.10\).aspx#BKMK\\_1](http://technet.microsoft.com/en-us/library/cc725767(v=ws.10).aspx#BKMK_1).

4 Connect to the AD LDS instance over LDAPS using *Ldp.exe*.

Follow the instructions in section "Step 3: Connect to the AD LDS instance over LDAPS using *Ldp.exe*" of the "Configuring LDAP over SSL Requirements for AD LDS" topic on [http://technet.microsoft.com/en-us/library/cc725767\(v=ws.10\).aspx#BKMK\\_1](http://technet.microsoft.com/en-us/library/cc725767(v=ws.10).aspx#BKMK_1).

5 Test the PTR record.

The view connection server needs to have a PTR record on the DNS server, which can be resolved on the Fglam server. To test a PTR record, use the command `ping -a IP`. The IP should be resolved to a FQDN.

For example, in Win2k8 R2:

- a Go to Start Menu > Administrative Tools > DNS, to open the DNS Manager.
- b Select and expand the target AD server, right click **Reverse Lookup Zones**, and select **New Zone** from the menu.

- c Follow the wizard to complete the configuration.

#### References:

- Configuring LDAP over SSL Requirements for AD LDS: [http://technet.microsoft.com/en-us/library/cc725767\(v=ws.10\).aspx#BKMK\\_1](http://technet.microsoft.com/en-us/library/cc725767(v=ws.10).aspx#BKMK_1)
- LDAP over SSL (LDAPS) Certificate: <http://social.technet.microsoft.com/wiki/contents/articles/2980.Ldap-over-ssl-ldaps-certificate.aspx>

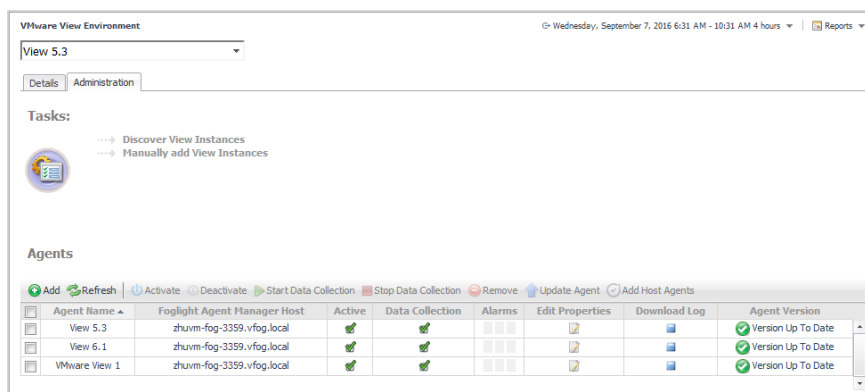
## Explore administrative tasks

The **Administration** tab of the VMware View Environment dashboard contains links to agent administration tasks that you can use to manage or create agent instances. From this tab, you can choose to either detect the agent instance information during creation or enter the information manually. Both methods create a View Connection Server Agent.

This tab consists of the **Tasks area** and the **Agents view**. Additional administrative tasks include:

- [Manually add View instances](#)
- [Discover View instances](#)
- [Add Host Agents](#)

Figure 7. VMware View Environment dashboard: Administration tab



## Tasks area

The **Tasks** area contains links to administrative tasks that you can initiate from this tab:

- **Discover View Instances.** Starts a workflow for detecting the agent information during creation. This information is detected by a Discovery Agent. This agent is responsible for gathering the server inventory information that is available for use by a View Connection Server Agent. For more information, see [Discover View instances](#).
- **Manually Add View Instances.** Starts a workflow for creating new agent instances. This workflow requires you to know the Connection Server and other domain-related details. For more information, see [Manually add View instances](#).

# Agents view

The **Agents** view shows a list of existing agent instances and a set of agent management buttons at the top of the list. The following buttons are available:

- **Add.** Starts a workflow for creating new agent instances. This workflow is the same as clicking the [Manually add View instances](#) link in the Tasks area.
  - **Refresh.** Refreshes the list of agent instances and their states.
  - **Activate.** Activates one or more selected agent instances. Activating an agent instance starts the agent process on the machine on which the agent is installed.
  - **Deactivate.** Deactivates one or more selected agent instances. Deactivating an agent stops the agent process on the machine on which the agent is installed.
  - **Start Data Collection.** Starts the data collection for one or more selected agent instances. Starting an agent's data collection causes the agent to begin monitoring a Connection Server, and to send the collected metrics back to the Management Server.
  - **Stop Data Collection.** Stops the data collection for one or more selected agent instances. Stopping an agent's data collection causes the agent to stop monitoring the Connection Server.
  - **Remove.** Deletes the selected agent instance.
  - **Update Agent.** Upgrades the agent to a new version, after a new cartridge is installed.
- i** **NOTE:** When a newer Foglight for VMware Horizon View version is installed on your system, the Agent Version column in the Agents table is updated to read *Update Agent*. To apply the new features, you need to update the agents to the latest version. You can upgrade the agents one by one, by selecting each from the table and clicking the corresponding *Update Agent* link in the Agent version column; you can upgrade all agents at once by selecting all of them in the list and clicking the **Update Agent** button at the top of the list.
- **Add Host Agents.** Starts a workflow for adding Infrastructure agents to monitor your VMware Horizon View environment. For more information, see [Add Host Agents](#).

To perform an agent management command, select one or more check boxes in the left-most column and click the appropriate button. For example, to start an agent's data collection, select the check box in the agent row and click **Start Data Collection**.

The table in the **Agents** area lists the existing View Connection Server Agent instances. For more details about the data appearing in this table, see [Agents view](#).

The **Download Log** button offers a convenient way to get the current log file of the corresponding agent, for review and diagnostics.

## To edit the properties of an instance:

- 1 Click the **Edit Properties** icon associated with that instance.  
The Edit Properties dialog box appears.
- 2 Modify the fields, as necessary:
  - **View Instance Name.** Name that you want to use for the view instance. This name becomes the name of the View Connection Server Agent, and appears in the drop-down list at the top left of the VMware View dashboards. The default name is **VMware View x**, where x is the next sequential number that is available.
  - **Connection Server.** Fully-qualified name of the Connection Server that is monitored by the View Connection Server Agent.
  - **User Name.** User name of the local host user (not the domain user) the agent uses to connect to the monitored host. This user can be a normal domain user, with privileges to view the environment.

**i** **NOTE:** To verify whether the user has proper view privileges, see [Connection server PowerShell configuration](#).

- **Password.** User password.
- **Domain Or Kerberos Realm.** Fully-qualified name of the domain to which the host on the Connection Server is running belongs.
- **Use DCom.** To use the DCOM collection method and the Kerberos authentication scheme, set the property to `True`. To use the WinRM collection method and the SSL authentication, set the property to `False`.
  - i | NOTE:** Foglight for VMware Horizon View uses two different methods for collecting data from remote hosts: Windows® Remote Management (WinRM) and Distributed Component Object Model (DCOM). For more information, see [Host configuration \(WinRM\)](#) and [Host configuration \(DCOM\)](#).
- **Use SSL.** To enable SSL set this property to `True`, to disable SSL set it to `False` (default is `False`).
  - i | NOTE:** When SSL is enabled, the **WS-Man CommunicationPort** is automatically set to 5986. When SSL is disabled, the **WS-Man CommunicationPort** is automatically set to 5985.
- **Authentication Scheme.** This property is set to `kerberos`. This is required for domain users.
- **WS-Man Communication Port.** Automatically set to 5986 if **Use SSL** is set to `True`; automatically set to 5985 if **Use SSL** is set to `False`.
- **WS-Man Additional URL.** The default value is `wsman`.
- **Event Database Password.** Event database password; must be the same as the one configured in VMware View Administrator (**View Configuration > Event Configuration**). When the password is specified, it enables the event-based rules in Foglight for VMware Horizon View. When no password is specified, the alarms from the event database are not logged.
  - i | NOTE:** The event database configuration, including the access password, is defined by the Event Database administrator during the event database installation and setup. For more information about this topic, refer to VMware® documentation.

### 3 Click **Save**.

The new settings are saved for the selected instance.

## Manually add View instances

Foglight for VMware Horizon View uses View Connection Server Agents to collect information from monitored environments. Creating a View Connection Server Agent instance creates the agent process on the Agent Manager host. Activating the View Connection Server Agent starts that agent process, while starting an agent instance's data collection enables the agent to start collecting data from the monitored View Connection Server and send it to Foglight for Hyper-V.

When the View Connection Server Agent package is successfully deployed, create one or more agent instances, activate them, and start their data collection. To perform these steps in a single operation for one or more monitored hosts, follow the procedure outlined below.

- i | NOTE:** This workflow is the same as clicking the Add button in the Agents area.

### **To create, activate View Connection Agent instances, and start their data collection:**

- 1 Log in to the Foglight browser interface. On the navigation panel, click **Dashboards > VMware View**.
- 2 On the VMware View Environment dashboard that appears in the display area, open the **Administration** tab.
- 3 In the **Tasks** area, click **Manually add View Instances**.

The Create View Agent wizard appears, showing the **Prepare** page. This page provides information about steps that need to be taken prior to proceeding with the wizard.

The two links at the bottom of the screen provide an easy way to download the scripts to automatically configure the View environment for monitoring, using DCom or WinRM, respectively.

The screenshot shows the 'Create View Agent' wizard with the 'Prepare' step selected. The left sidebar lists the steps: Prepare, Select An Agent Host, Agent Properties, Connectivity Diagnostic, and Connectivity Diagnostic Result. The main area contains instructions: 'Before continuing with this wizard, it is **critical** that the Connection Servers to be monitored are configured correctly. To see more details about prerequisites and configuration, please click the **i** in the top right corner.' Below this, it says 'To download a script to automatically configure, click one of the following links:' followed by two links: 'Script for DCom setting.' and 'Script for WinRM setting.' At the bottom are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'.

- 4 Read the instructions and if the environment is configured correctly, click **Next**.

The **Select An Agent Host** page appears. This page shows a list containing one or more Agent Manager instances that can be used to collect data.

The screenshot shows the 'Create View Agent' wizard with the 'Select An Agent Host' step selected. The left sidebar lists the steps: Prepare, Select An Agent Host, Agent Properties, Connectivity Diagnostic, and Connectivity Diagnostic Result. The main area contains the instruction: 'Select the Foglight Agent Manager host for a new View Connection Server Agent.' Below this is a table with the following data:

Host Name	FglAM Version	OS	Architecture
10.10.10.10	5.9.5	windows	x86_64

At the bottom are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'.

- 5 Select an Agent Host and click **Next**.

The screenshot shows the 'Create View Agent' wizard with the 'Agent Properties' step selected. The left sidebar lists the steps: Prepare, Select An Agent Host, Agent Properties, Connectivity Diagnostic, and Connectivity Diagnostic Result. The main area contains the instruction: 'Enter the properties of the VMWare View to access it.' Below this are several input fields and radio buttons:

- View Instance Name: VMware View 4
- Connection Server:
- User Name:
- Password:
- Domain Or Kerberos Realm:
- Use DCom: ☐ True ☒ False
- Use SSL: ☐ True ☒ False
- Authentication Scheme: kerberos
- WS-Man CommunicationPort: 5985
- WS-Man Additional URL: wsman
- Event Database Password:

At the bottom are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'.



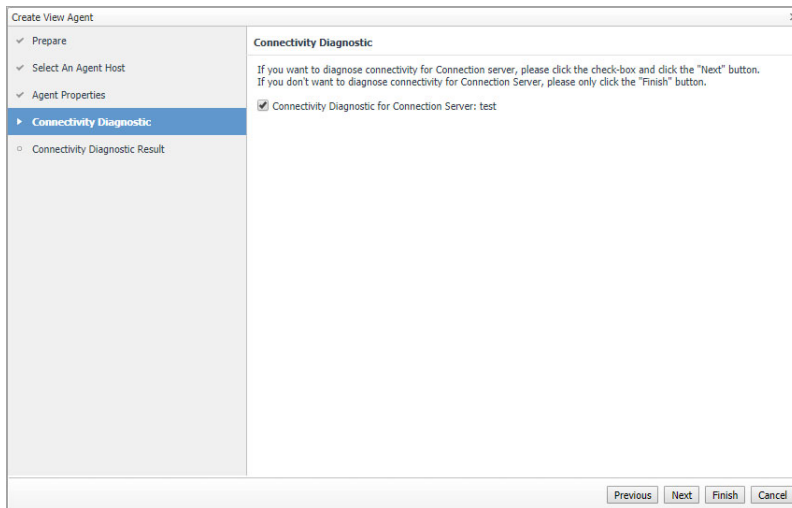
6 On the **Agent Properties** page, enter the following:

- **View Instance Name.** Name that you want to use for the view instance. This name becomes the name of the View Connection Server Agent, and appears in the drop-down list at the top left of the VMware View dashboards. The default name is **VMware View x**, where x is the next sequential number that is available.
- **Connection Server.** Fully-qualified name of the Connection Server that is monitored by the View Connection Server Agent.
- **User Name.** User name of the local host user (not the domain user) the agent uses to connect to the monitored host. This user can be a normal domain user, with privileges to view the environment.
  - **NOTE:** To verify whether the user has proper view privileges, see [Connection server PowerShell configuration](#).
- **Password.** User password.
- **Domain Or Kerberos Realm.** Fully-qualified name of the domain to which the host on the Connection Server is running belongs.
- **Use DCom.** To use the DCOM collection method and the Kerberos authentication scheme, set the property to `True`. To use the WinRM collection method and the SSL authentication, set the property to `False`.
  - **NOTE:** Foglight for VMware Horizon View uses two different methods for collecting data from remote hosts: Windows® Remote Management (WinRM) and Distributed Component Object Model (DCOM). For more information, see [Host configuration \(WinRM\)](#) and [Host configuration \(DCOM\)](#).
- **Use SSL.** To enable SSL set this property to `True`, to disable SSL set it to `False` (default is `False`).
  - **NOTE:** When SSL is enabled, the **WS-Man CommunicationPort** is automatically set to 5986. When SSL is disabled, the **WS-Man CommunicationPort** is automatically set to 5985.
- **Authentication Scheme.** This property is set to `kerberos`. This is required for domain users.
- **WS-Man Communication Port.** Automatically set to 5986 if **Use SSL** is set to `True`; automatically set to 5985 if **Use SSL** is set to `False`.
- **WS-Man Additional URL.** The default value is `wsman`.
- **Event Database Password.** Event database password; must be the same as the one configured in VMware View Administrator (**View Configuration > Event Configuration**). When the password is specified, it enables the event-based rules in Foglight for VMware Horizon View. When no password is specified, the alarms from the event database are not logged.
  - **NOTE:** The event database configuration, including the access password, is defined by the Event Database administrator during the event database installation and setup. For more information about this topic, refer to VMware® documentation.

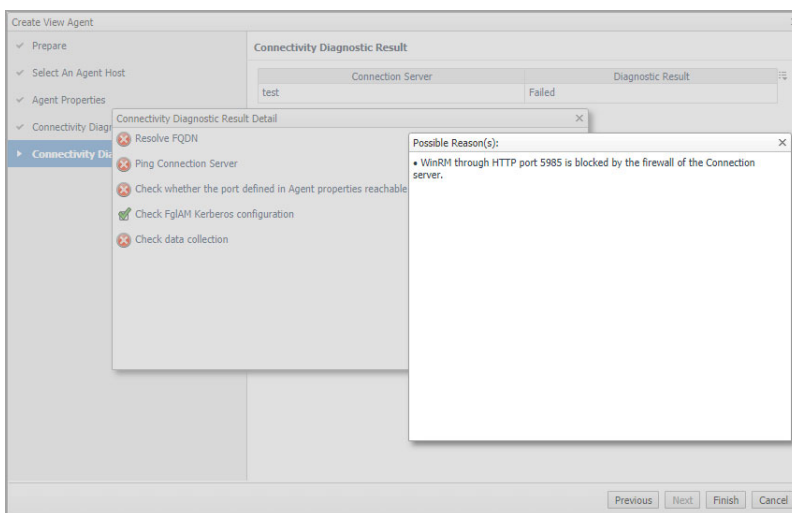
Click **Next**.

7 On the **Connectivity Diagnostic** page

- If you want to diagnose connectivity for Connection server, click the check-box and **Next**.
- If you don't want to diagnose connectivity for Connection server, click **Finish**.

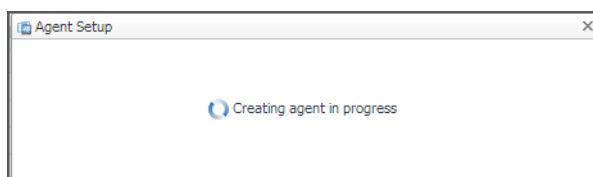


- 8 Wait for a few seconds until the **Connectivity Diagnostic Result** page appears. Click the Diagnostic Result and the **Connectivity Diagnostic Result Detail** page appears. Click on the failed items to see the possible reasons.

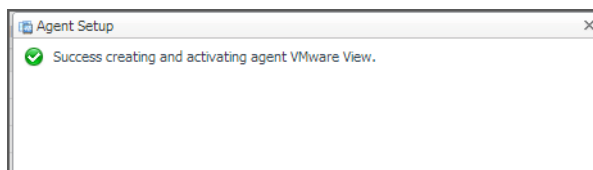


- 9 Click **Finish** after connectivity diagnostic completes.

A progress message appears.



When the agent is created, a message indicating successful completion appears.



The **Administration** tab refreshes, showing the newly created instance of the View Connection Server Agent in the list.

The agent is activated and data collection starts.

- 10 If required, configure configuration or data collection properties for one or more agents.

When a View Connection Server Agent connects to the Management Server, it is provided with sets of properties that it uses to configure its correct running state. Foglight for Hyper-V stores agent properties on the Management Server.

- a Select the agent whose connection properties you want to edit and click **Edit Properties**.

The **Edit Properties** dialog box appears.

- b Edit the agent properties as required and click **Save**.

**i** **NOTE:** To quickly edit the properties for all View Connection Server agents at once, use the Agent Status dashboard (Administration > Agents > Agent Status). For more information on this dashboard, see the *Foglight Administration and Configuration Guide*.

## Discover View instances

This workflow discovers the server information that is available in your View environment and automatically enters it into the Wizard screens. After running the Wizard, a Discovery Agent is created.

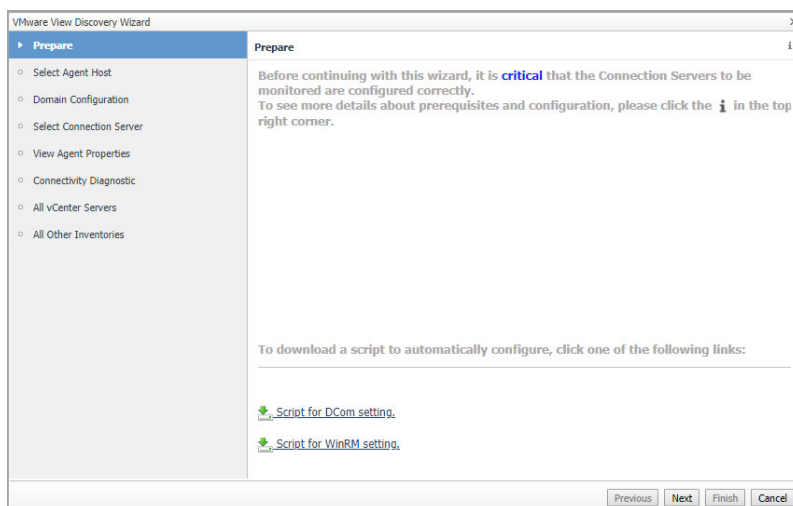
**i** **NOTE:** The Discovery Agent is not listed in the Agents table. Instead, it is listed in the Agent Status dashboard (Administration > Agents > Agent Status). The agent name is VMView-ConnServer-Discovery. You can edit and modify its properties as you would any other View Connection Server agent. For more information on working with the Agent Status dashboard, see the *Foglight Administration and Configuration Guide*.

### To create, activate View Connection Agent instances, and start their data collection:

- 1 Launch the **Discover View Instances** wizard located in the **Tasks** area.

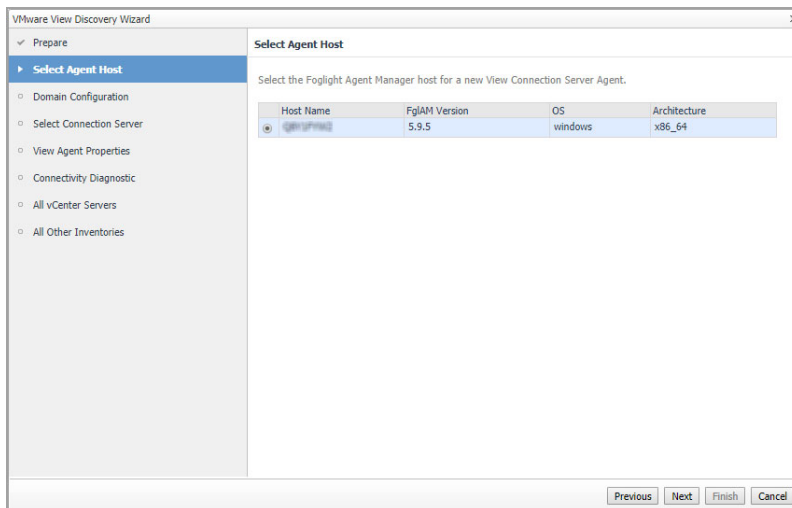
The **VMware View Discovery** wizard appears, showing the **Prepare** page. This page provides informations about steps that need to be taken prior to proceeding with the wizard.

The two links at the bottom of the screen provide an easy way to download the scripts to automatically configure the View environment for monitoring, using DCom or WinRM, respectively.



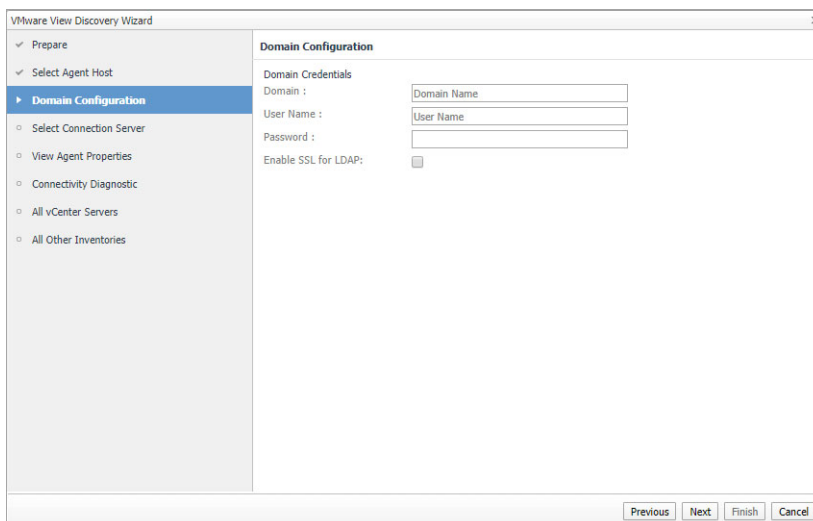
- 2 Read the instructions and if the environment is configured correctly, click **Next**.

The **Select Agent Host** page appears. The Foglight Agent Manager host information listed on the page is from the Agent Host dashboard (**Administration > Agents > Agent Hosts**).



- 3 Select the Foglight Agent Manager Host to be used for the new View Connection Server agent instance, then click **Next**.

The **Domain Configuration** page appears.



- 4 Enter the following:
  - **Domain.** Fully-qualified name of a domain to search for the View Connection Server. For example, myDomain.com.
  - **User Name.** User name of an account in the domain.
 

**NOTE:** To verify whether the user has proper view privileges, see [Connection server PowerShell configuration](#).
  - **Password.** Password associated with the above user name.
  - **Enable SSL for LDAP.** Select this option to enable SSL for LDAP connection.
 

**NOTE:** In FIPS-compliant mode, you need to import the CA certificate or the self-signed certificate to the KeyStore of FglAM to use this option. For more information, see [Managing certificates for FglAM](#) on page 36.
- 5 Click **Next**.

The Select Connection Server page appears. It includes a list of all Connection Servers to which you have access, based on the domain name and user credentials that you entered in the previous step.

If the wizard cannot retrieve any connection servers, an error message is displayed instead of the Connection Servers list. You can try again or manually fill in a FQDN (by selecting the **Other Connection Server (FQDN)** check box and filling the FQDN name in the text box), then proceed to the next wizard page. Continue with the instructions on [Step 7](#).

- 6 Select the Connection Server that you want to monitor in the agent instance. When you select a Connection Server, the **AD's credential** check box is automatically selected, and the **User Name** and **Password** boxes are pre-filled based on the user name and password that you entered in [Step 4](#). The **Other Connection Server (FQDN)** text box is pre-filled with the DNS name. Modify these entries as required.
- 7 Click **Next**.
- 8 On the **View Agent Properties** page, provide the following information:

- **View Instance Name.** Name that you want to use for the view instance. This name becomes the name of the agent, and appears in the drop-down list at the top left of the VMware View dashboards. The default name is **VMware View x**, where x is the next sequential number that is available.
  - ❗ **NOTE:** The Connection Servers, user name and password, and domain are already pre-populated based on the information you entered in [Step 4](#).

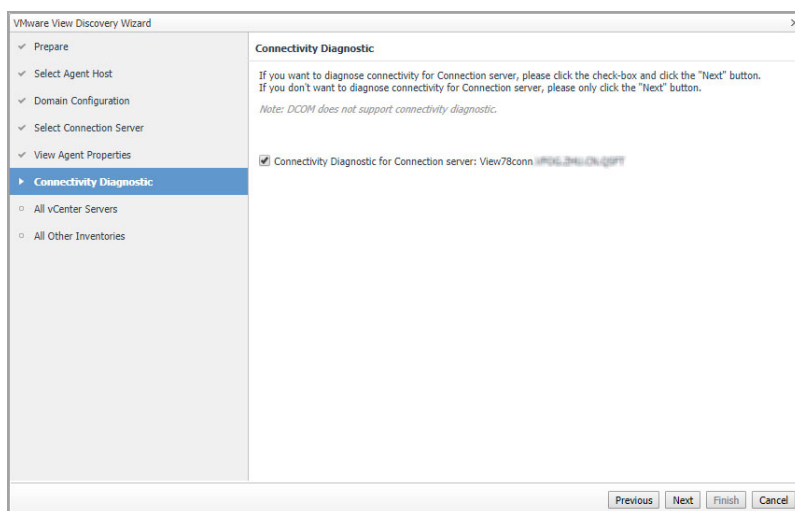
- **Use DCOM.** To use the DCOM collection method and the Kerberos authentication scheme, set the property to `True`. To use the WinRM collection method and the SSL authentication, set the property to `False`.
  - **NOTE:** Foglight for VMware Horizon View uses two different methods for collecting data from remote hosts: Windows® Remote Management (WinRM) and Distributed Component Object Model (DCOM). For more information, see [Host configuration \(WinRM\)](#) and [Host configuration \(DCOM\)](#).
- **Use SSL.** To enable SSL set this property to `True`, to disable SSL set it to `False` (default is `False`).
  - **NOTE:** When SSL is enabled, the **WS-Man CommunicationPort** is automatically set to 5986. When SSL is disabled, the **WS-Man CommunicationPort** is automatically set to 5985.
- **WS-Man Communication Port.** Automatically set to 5986 if **Use SSL** is set to `True`; automatically set to 5985 if **Use SSL** is set to `False`.
- **WS-Man Additional URL.** Set this property to `wsman` (default setting).
- **Event Database Password.** Event database password; must be the same as the one configured in VMware View Administrator (**View Configuration > Event Configuration**). When the password is specified, it enables the event-based rules in Foglight for VMware Horizon View. When no password is specified, the alarms from the event database are not logged.
  - **NOTE:** The event database configuration, including the access password, is defined by the Event Database administrator during the event database installation and setup. For more information about this topic, refer to VMware® documentation.

The following fields are pre-filled with the appropriate information:

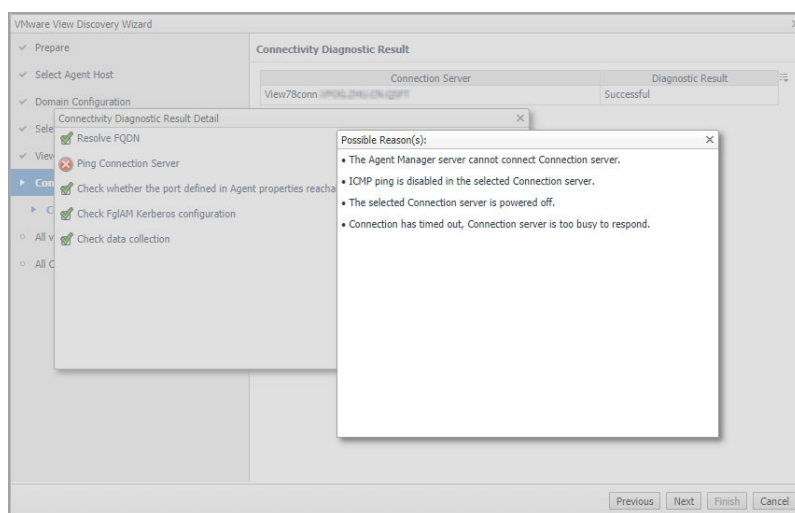
- **Connection Server.** Fully-qualified name of the Connection Server that is monitored by the View Connection Server Agent.
- **User Name.** User name of the local host user (not the domain user) the agent uses to connect to the monitored host. This user can be a normal domain user, with privileges to view the environment.
  - **NOTE:** To verify whether the user has proper view privileges, see [Connection server PowerShell configuration](#).
- **Password.** User password.
- **Domain / Kerberos Realm.** Fully-qualified name of the domain to which the host on the Connection Server is running belongs.
- **Authentication Scheme.** This property is set to `kerberos`. This is required for domain users.

#### 9 Click **Next**.

The **Connectivity Diagnostic page** appears. If you want to diagnose connectivity for Connection server, click the check-box and **Next**. If you don't want to diagnose connectivity for Connection server, click **Next**.

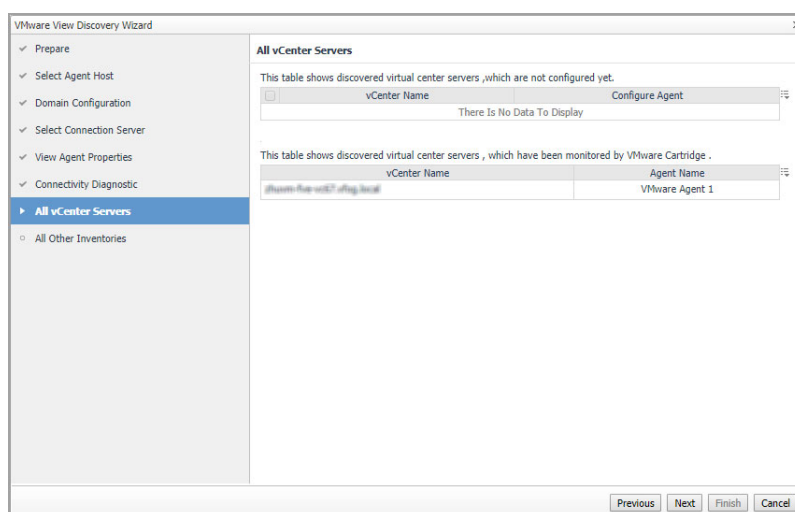


- 10 Wait for a few seconds until the **Connectivity Diagnostic Result** page appears. Click the Diagnostic Result and the **Connectivity Diagnostic Result Detail** page appears. Click on the failed items to see the possible reasons.



- 11 Click **Next**.

The **All vCenter Servers** page appears, listing the vCenter® servers in the domain.



- The top table lists the vCenter servers for which the agent is not configured yet. To configure a VMware® agent to monitor a vCenter server, click the icon in the *Configure Agent* column. The **VMware vCenter Agent: Configure Agent Properties** dialog box appears.

Fill in the port and credential information for creating the VMware® agent, then click **Save**. For detailed information about configuring VMware agents, see the *Managing Virtualized Environments User and Reference Guide*.

- The lower table lists the vCenter servers which are already monitored by Foglight for VMware.

12 Click **Next**.

The **All Other Inventories** page appears. This page lists the terminal servers, security servers, and connection servers that are in the VMware View infrastructure.

- 13 Select those servers for which you want to create an Infrastructure (IC) Agent. The agent will monitor the selected servers.

Type	Host Name	Dns Name
<input type="checkbox"/> Connection Server	VIEW70CONN	View70Conn.vic.local
<input type="checkbox"/> Connection Server	VIEW78CONN	View78Conn.vic.local
<input type="checkbox"/> Composer Server	view78comp	view78comp.vic.local

**NOTE:** It is recommended that you create an IC agent to monitor your VMware Horizon View environment. An IC agent collects data such as CPU, disk, memory, services, and other network metrics for the VMware Horizon View components in your environment. This data appears on the Details tab of the VMware View Environment dashboard. For more information, see the *Managing Infrastructure User and Reference Guide*.

- 14 Click **Finish** after connectivity diagnostic completes.

When the agent is created, a message indicating successful completion appears.

## Add Host Agents

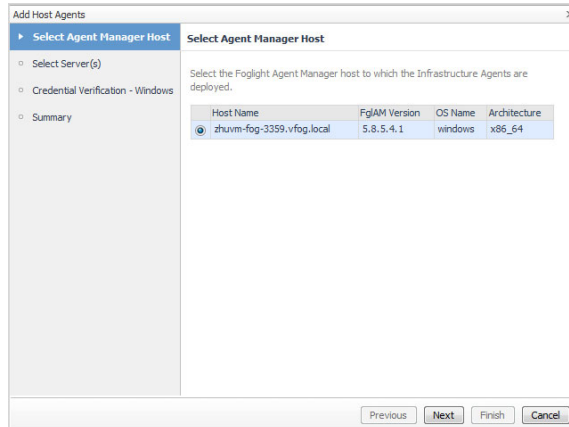
This workflow allows you to add Infrastructure (IC) agents to monitor your VMware Horizon View environment. An IC agent collects data such as CPU, disk, memory, services, and other network metrics for the VMware Horizon View components in your environment. This data appears on the Details tab of the VMware View Environment dashboard.



### To add an Infrastructure agent:

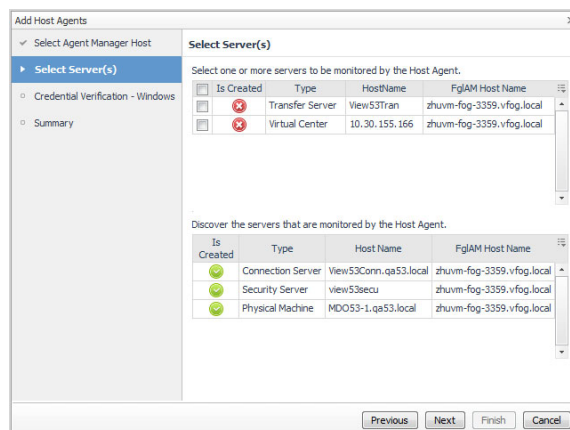
- 1 In the VMware View Environment dashboard > Administration tab > Agents view, select a View agent instance from the list, then click **Add Host Agents**.

The Add Host Agents wizard appears, showing the **Select Agent Manager Host** page. The information listed on this page is from the Agent Host dashboard (Administration > Agents > Agent Hosts).



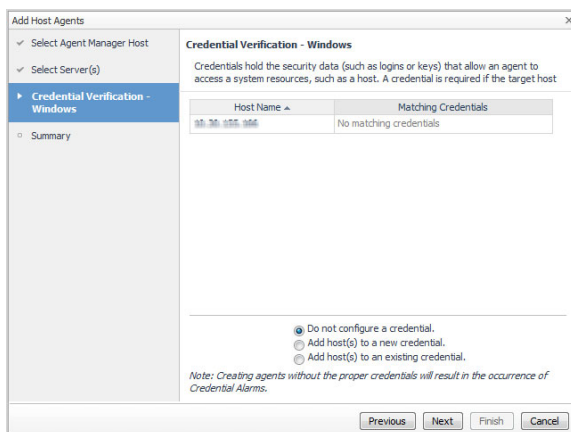
- 2 Select the Foglight Agent Manager Host to be used for the new Infrastructure agent instance, then click **Next**.

The **Select Server(s)** page appears. This page lists the terminal servers, security servers, and connection servers that are in the VMware View infrastructure.



- 3 Select those servers for which you want to create an Infrastructure (IC) Agent, then click **Next**. The agent will monitor the selected servers.

The **Credential Verification - Windows** page appears. Credentials are security data that provide the Infrastructure agents with the permission to monitor system resources, such as a host or a range of hosts.



4 Select one of the following options:

- **Do not configure a credential.** Select this option if you want to configure the credential for this resource at a later time. Local credentials for Windows® and UNIX® are set up by default when Foglight for Infrastructure is installed. Click **Next** and continue with [Step 7](#).
- **Add host(s) to a new credential.** Select this option if you want to add the host to a new credential. This option is suitable if none of the existing credentials have the connection details needed to access the new host. Click **Next** and continue with [Step 5](#).
- **Add host(s) to an existing credential.** Select this option if you want to add the host to an existing credential. This option is suitable if an existing credential has the security data needed to access the new host, but you need to edit its resource mappings to include this host. Click **Next** and continue with [Step 6](#).

5 Create a new credential.

- a On the **Credential Type** page that appears, select the credential type from the available options.
- b Click **Next**.

The **Credential Properties** page appears. The level of required information depends on the selected credential type. For example, the **User Name and Password** type needs a user name and a password, while the **Challenge Response** type needs a user name along with a question/response pair.

- c On the **Credential Properties** page, type the required properties, and click **Next**.

The **Credential Name and Lockbox** page appears.

- d On the **Credential Name and Lockbox** page, provide a name to identify the credential, and select a lockbox in which you want to keep the credential. A lockbox can be used to group credentials for access and/or security. In smaller Foglight installations, using the default **System** lockbox should be sufficient.

**i** | **NOTE:** If a lockbox is password protected and is not released to the target Foglight Agent Manager, you can provide the lockbox password on the last page of the wizard.

Click **Next**.

The **Resource Mapping** page appears.

- e On the **Resource Mapping** page, indicate which hosts you want to associate with this credential. You can either select the host that you are about to start monitoring, all monitored hosts, or hosts whose name contains a specific text string.

Click **Next**.

The **Policies** page appears.

- f Optional. On the **Policies** page, define one or more policies for this credential. A policy defines the number of times a credential can be used, the number of allowed authentication failures, the time

range during which the credential is valid, or the length of time the credential data can be cached on the client. For example, you can specify the number of times the credential can be used, or the time period during which it can be used. For complete information about the available credential policies, see the *Foglight Administration and Configuration Help*.

Click **Next**.

The **Summary** page appears.

- g Continue with [Step 7](#).

## 6 Use an existing credential.

- a On the **Credential** page that appears, select an existing credential to contain this host.
- b Click **Next**.

The **Resource Mapping** page appears.

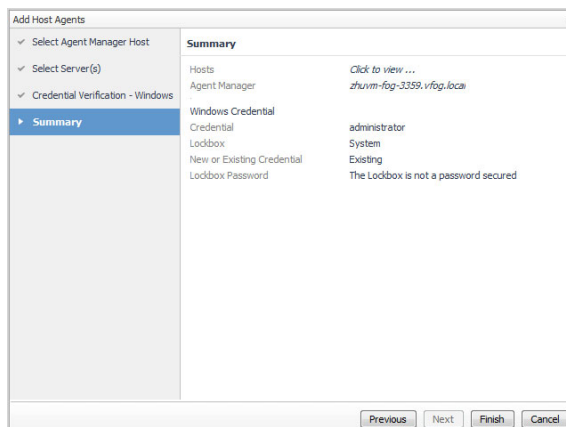
- c On the **Resource Mapping** page, indicate which hosts you want to associate with this credential. You can either select the host that you are about to start monitoring, all monitored hosts, or hosts whose name contains a specific text string.

Click **Next**.

The **Summary** page appears.

- d Continue with [Step 7](#).

## 7 On the **Summary** page that appears, review the information provided about the host and the monitoring agent.



## 8 Click **Finish**.

The new host is added to the **Hosts** dashboard after a short delay. The monitoring agent is created.

If the operation is successful, the **Result For Agent(s) Creation** dialog box appears. Review the information and close the dialog box.

The agent instance created to monitor the new host appear on the **Administration > Agents > Agent Status** dashboard.

# Managing certificates

## Syntax Conventions

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

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

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

`C:\Quest\Foglight_Agent_Manager`

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

`C:\Quest\Foglight\fglam`

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

## Managing certificates for FglAM

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

### Prerequisite

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

### Add a certificate

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

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

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

**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 FMS in FIPS-compliant mode

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

The KeyStore Foglight used in FIPS-compliant mode is located at:

`<Foglight_home>/config/security/trust.fips.keystore` (default password: nitrogen)

### Add a certificate in FIPS-compliant mode

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

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

- Validate the certificate and ensure the following:
  - It is not expired.
  - It is an X.509 format.
- Change the following before executing the command

- `<alias>`: The alias is required and is used in the list and delete operations to refer to the certificate. It can be anything.
- `<Foglight_home>`: The folder path where Foglight is installed.
- `<certificate path>`: Your custom certificate path.

## List installed certificates

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

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

Refer to the example output below:

```
Keystore type: BCFKS
Keystore provider: BCFIPS
Your keystore contains 151 entries
camerfirmachambersignca [jdk], Dec 18, 2019, trustedCertEntry,
Certificate fingerprint (SHA1):
4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C
entrust2048ca [jdk], Dec 18, 2019, trustedCertEntry
...
```

## Delete a certificate

Remove a certificate referred to by an alias.

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

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

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

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

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

Extensions:
...

Trust this certificate? [no]: yes
```

Certificate was added to keystore

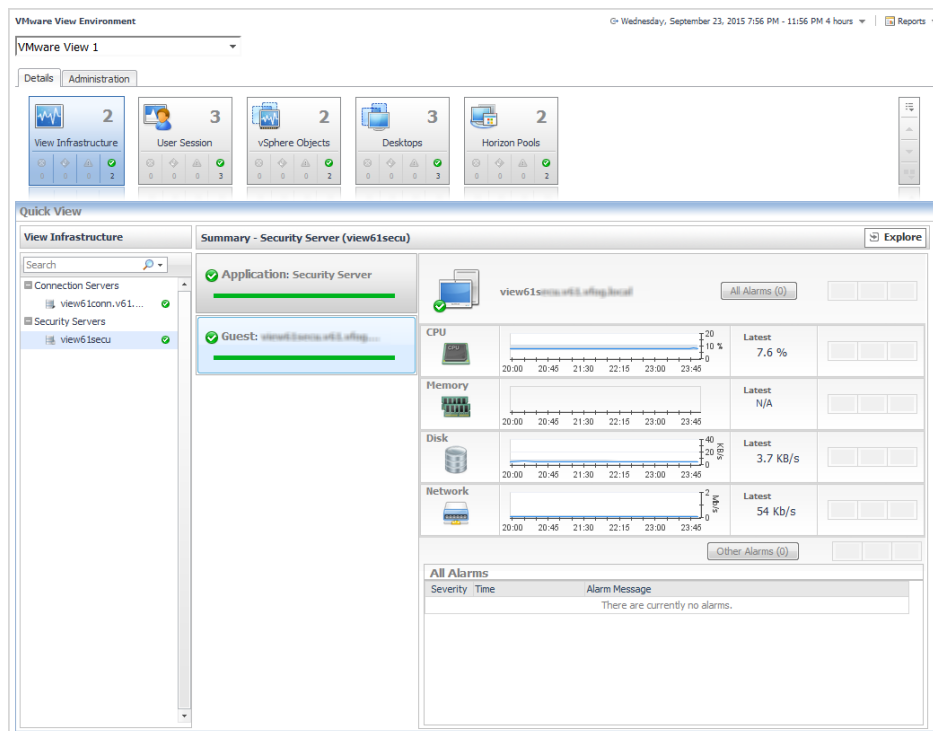
# Use the VMware View Environment dashboard

A typical VMware View environment contains a combination of physical and virtual components. A physical component can be a Connection Server, Terminal server, or a user desktop. You can view the overall state of all VMware View components on the VMware View Environment dashboard.

## To access the VMware View Environment dashboard:

- 1 Log in to the Foglight for Hyper-V browser interface.
- 2 Ensure that the navigation panel is open.  
To open the navigation panel, click the right-facing arrow on the left.
- 3 On the navigation panel, under **Dashboards**, choose **VMware View**.  
The **Details** and **Administration** tabs are available for selection.

Figure 8. VMware View Environment dashboard



For more information, see these topics:

- [Details tab](#)
- [Administration tab](#)
- [Navigating between View server instances](#)

## Details tab

The Details tab contains the Details view and the Quick View. Selecting an object type and its alarm state in the Details view shows the summary information for your selection in the [Quick View](#). For more information about the data appearing on this dashboard, see [Explore the VMware View Environment Details tab](#).

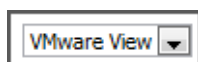
## Administration tab

You can use this tab to configure and administer View Connection Server agents to collect data from your monitored environment. For more information, see [Explore administrative tasks](#).

## Navigating between View server instances

Choosing a specific View server instance from the drop-down list in the top-left refreshes the VMware View Environment dashboard with the information about the selected environment.

Figure 9. View selector



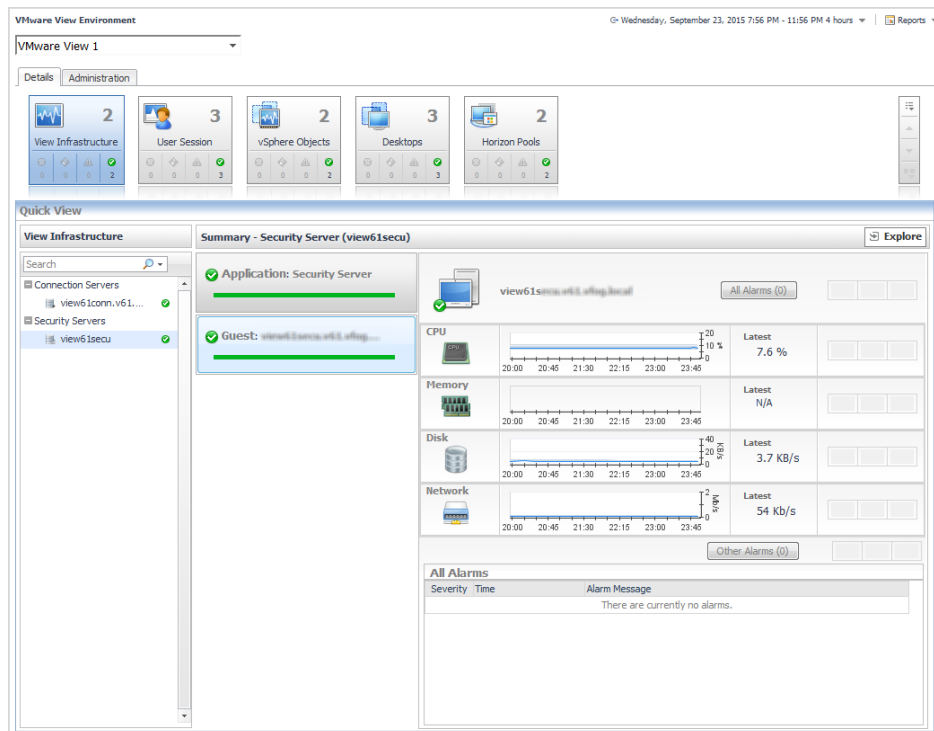
The list of View servers is populated from the View Instance Name that you create during agent creation. Each View Server instance can contain a different combination of monitored components. For more information on agent creation, see [Manually add View instances](#).

## Explore the VMware View Environment Details tab

The **VMware View Environment Details** tab contains tiles that summarize status. Selecting a tile changes the content displayed in the Quick View area. This content varies depending on the tile that you select. For example, selecting the **View Infrastructure** tile displays the connection server, terminal server, and security server details associated with a View Server instance.



Figure 10. VMware View Environment Details tab



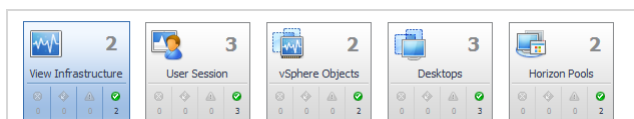
For more information, see these topics:

- [Work with tiles](#)
- [Use the Quick View](#)
- [Explore user sessions](#)
- [Explore desktops](#)
- [Explore Horizon Pools](#)

## Work with tiles

The upper part of the tile displays the desktop management component and a total count of these entries in the environment.

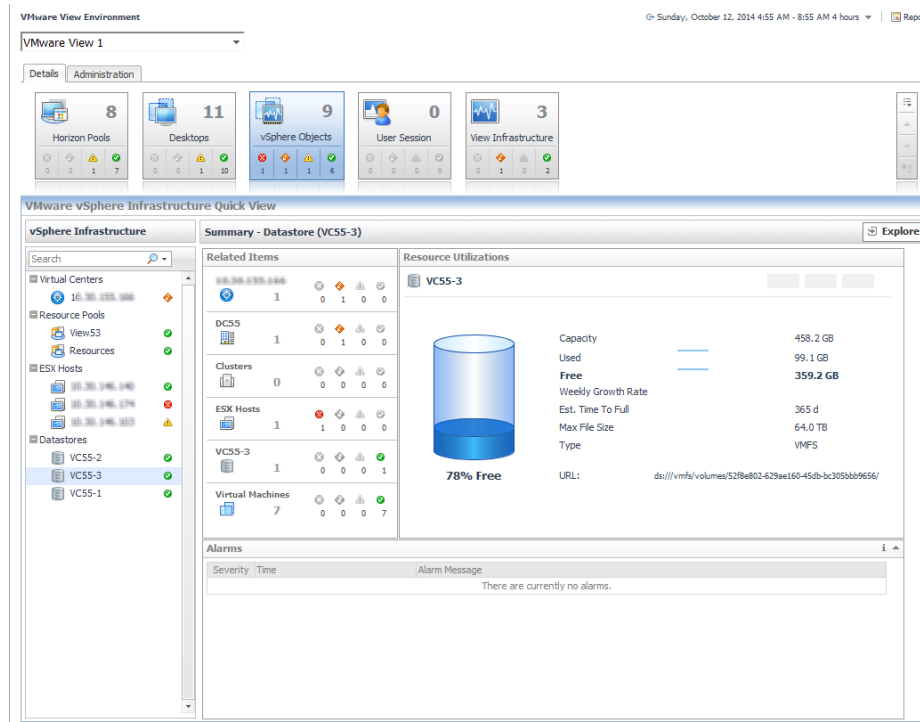
Figure 11. VMware View Environment tiles



The lower part of the tile displays the count of entities at each severity level, based on the alarms currently active for those entries.

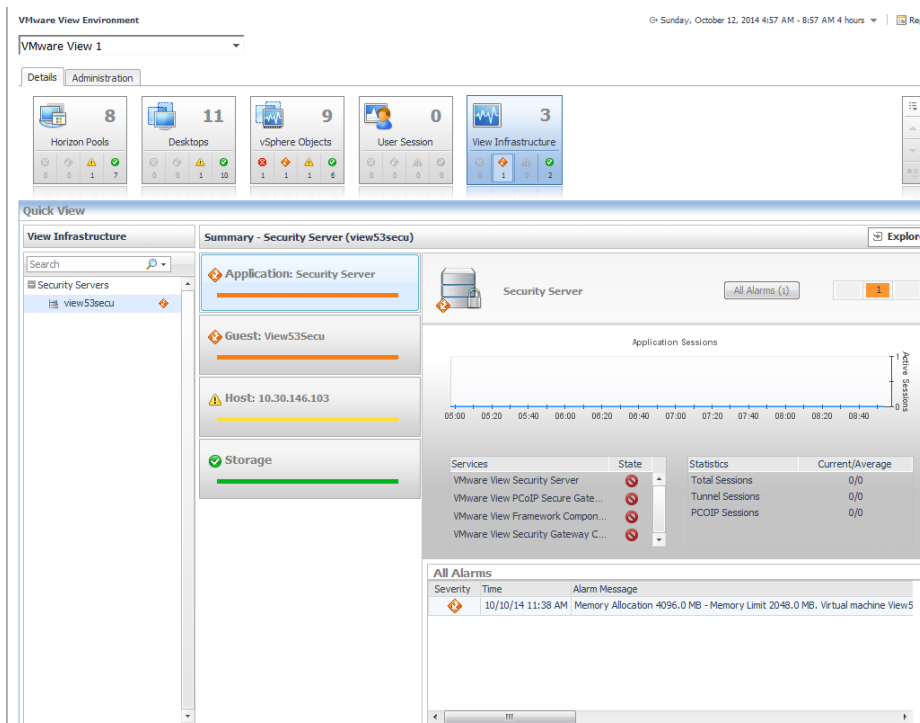
Clicking the label in the tile, for example, **vSphere Objects**, displays summary and alarm information for all components of that type in the Quick View area.

**Figure 12. VMware View Environment: Quick View**



Clicking the alarm count in the lower part of the tile displays summary and alarm information for only the components with that status.

**Figure 13. VMware View Environment: alarms displayed in Quick View**



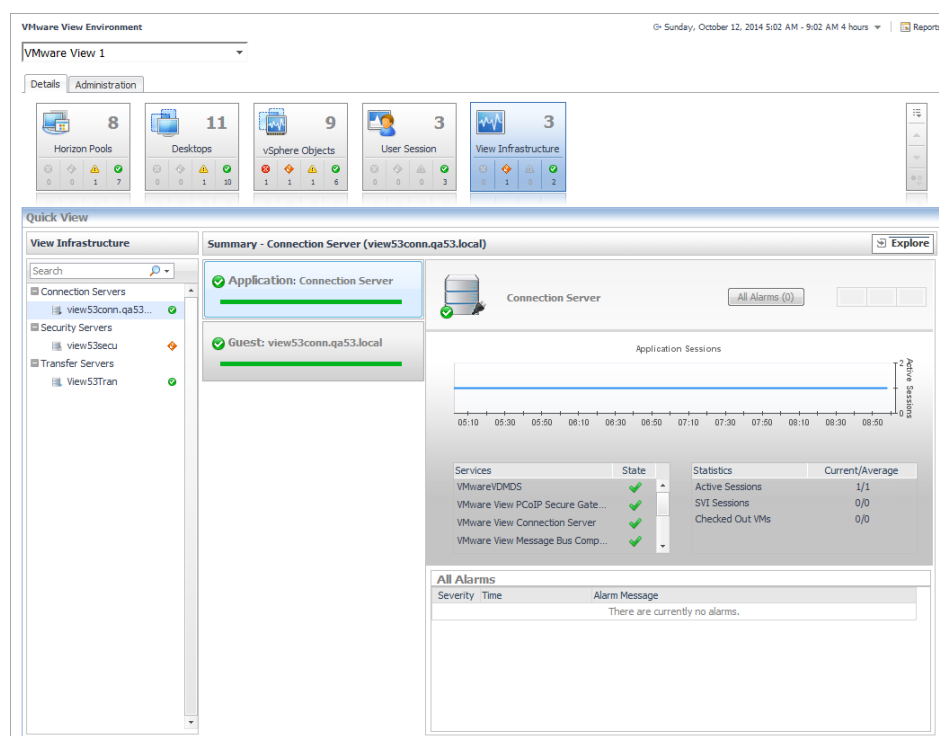
# Use the Quick View

Selecting a specific object in the navigation panel displays key summary information about child component health, resource utilization, and alarms.

Click the **Explore** link in the upper-right corner to drill down to the VMware Explorer view of the object, to see detailed information about the selected object and its components. If the selected object is a monitoring VM, the VMware Explorer page appears. For further information, see [Use the VMware Explorer](#). If the selected object is a host, the Host Monitor page appears.

**NOTE:** The **Explore** link applies to infrastructure components only. The components that appear in the User Session tile have their own Explore link. For more information, see [Explore user sessions](#).

Figure 14. Quick View



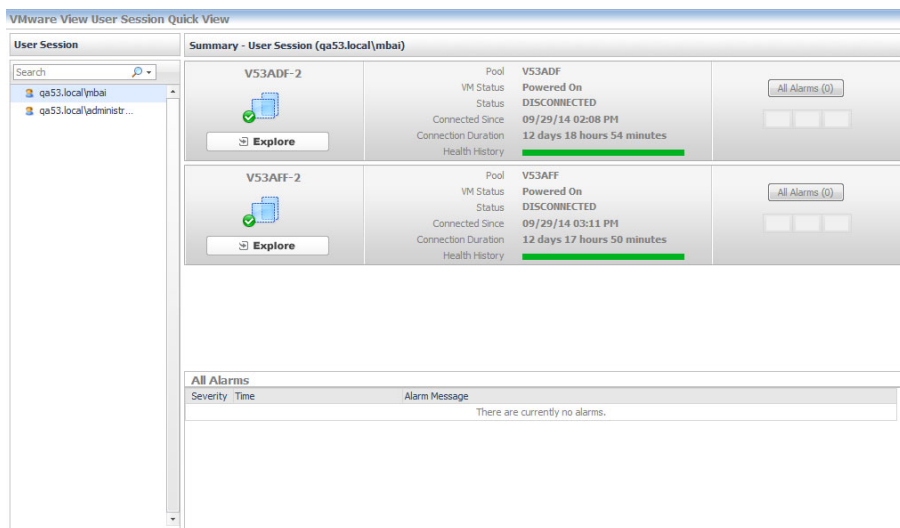
## Explore user sessions

When you click the **User Session** tile, a list of the connected users is shown in the Quick View. Selecting a user from the Quick View displays the session types for the user, and a summary of the session details depending on the session type. Each user will have one or more sessions in a View instance.

An **Explore** link is located below the icon of the session type. Click the link to view detailed information about the session type.

The All Alarms table at the bottom of the view shows all the alarms triggered for the user session.

Figure 15. Exploring user sessions



## Explore desktops

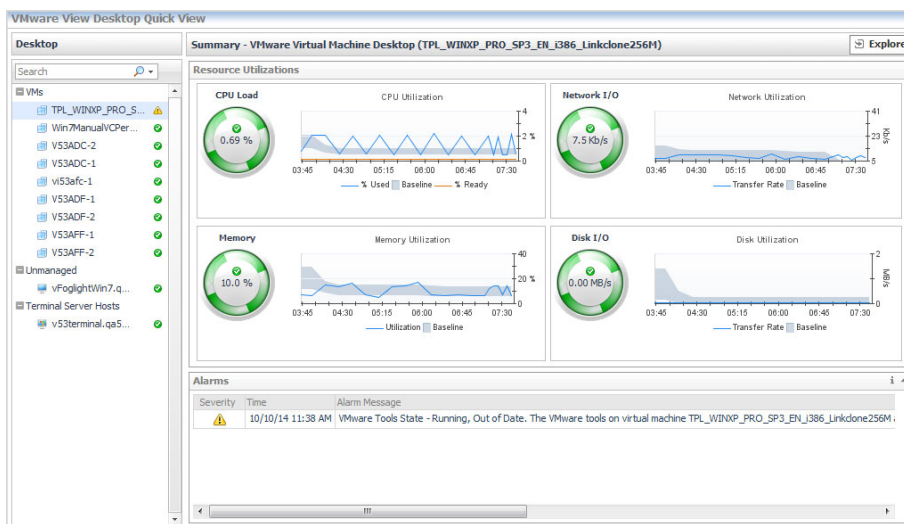
When you click the **Desktops** tile, a list of Virtual Machines, Terminal Service Hosts, and Unmanaged Desktops on Physical Hosts is displayed in the Quick View.

**NOTE:** Desktops on physical machines, including desktops of a physical host and desktop of a VM on a physical host are classified as “Unmanaged Desktops”.

Selecting a Virtual Machine from the Quick View list displays the resource utilization values for that VM in the Summary pane. Click the **Explorer** link in the upper-right corner to drill down to the VMware Explorer view of the object, to see detailed information about the selected object and its components. If the selected object is a monitoring VM, the VMware Explorer page appears. For more information, see [Use the VMware Explorer](#).

The Alarms table at the bottom of the view shows all the alarms triggered for the selected Virtual Machine.

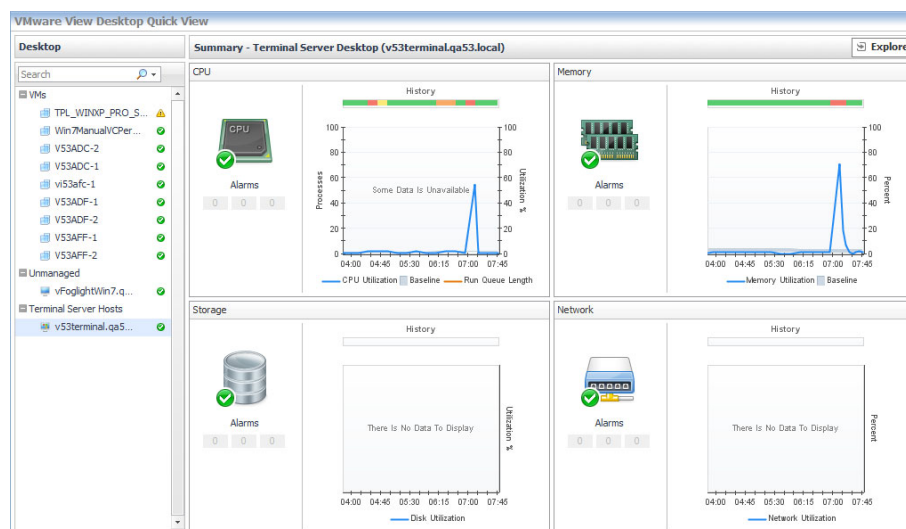
Figure 16. VMware Explorer page



Selecting a Terminal Service Host or an Unmanaged Desktop on Physical Host from the Quick View list displays the CPU, Memory, Network, and Storage utilization charts for the selected host in the Summary pane. Clicking any data series on the charts allows you to drill down into the Metric Analyzer dashboard for the associated metric and

view the metrics collected for that topology object. Click the **Explorer** link in the upper-right corner to drill down to the Host Monitor page for the selected host.

**Figure 17. Host Monitor page**



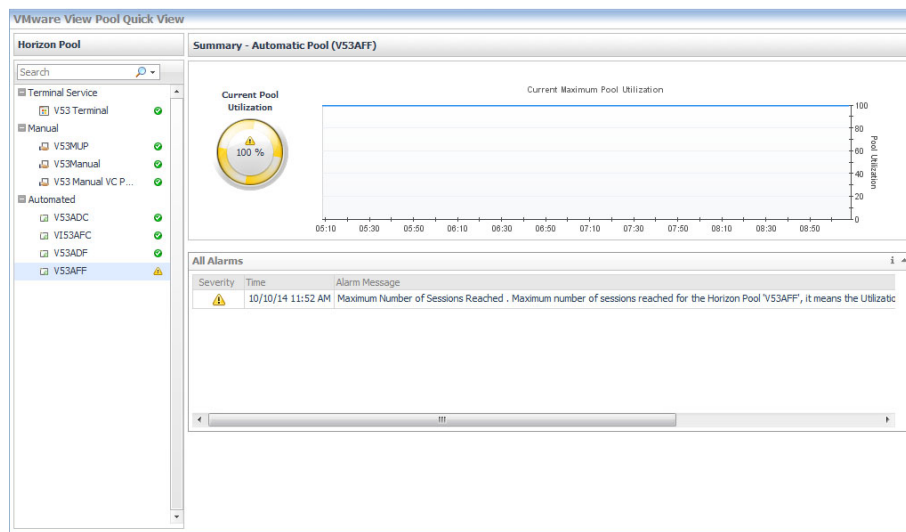
## Explore Horizon Pools


When you click the **Horizon Pools** tile, the Quick View shows a list of pools available in the View Instance. The pools are grouped by type: Automated, Manual, and Terminal Services.

When selecting a pool on the Quick View list, the Summary pane displays the following information for the selected pool:

- Pool name and type
- For Automated and Manual pools: the current maximum number of sessions possible and a chart of session utilization percentage
- For Terminal Services pools: a chart of session count
- All Alarms table showing all the alarms triggered for the pool

Figure 18. Exploring Horizon Pools

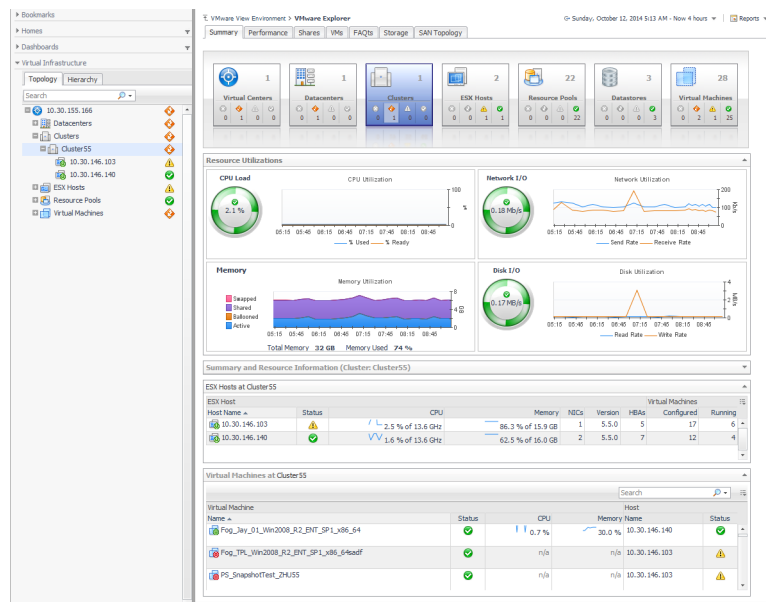


**NOTE:** The icon  in the Quick View tree indicates a pool that is disabled.

## Use the VMware Explorer

The VMware Explorer allows you to monitor a wide range of elements in your virtual infrastructure. It contains a number of informative views through which you can quickly and easily access detailed information about any of the available components (physical or virtual) within the infrastructure. Its hierarchical interface includes drilldown capabilities that display various performance metrics and alarms within the virtual infrastructure.

Figure 19. VMware Explorer



For reference information about the data appearing on this dashboard, see [VMware Explorer Primary view](#).

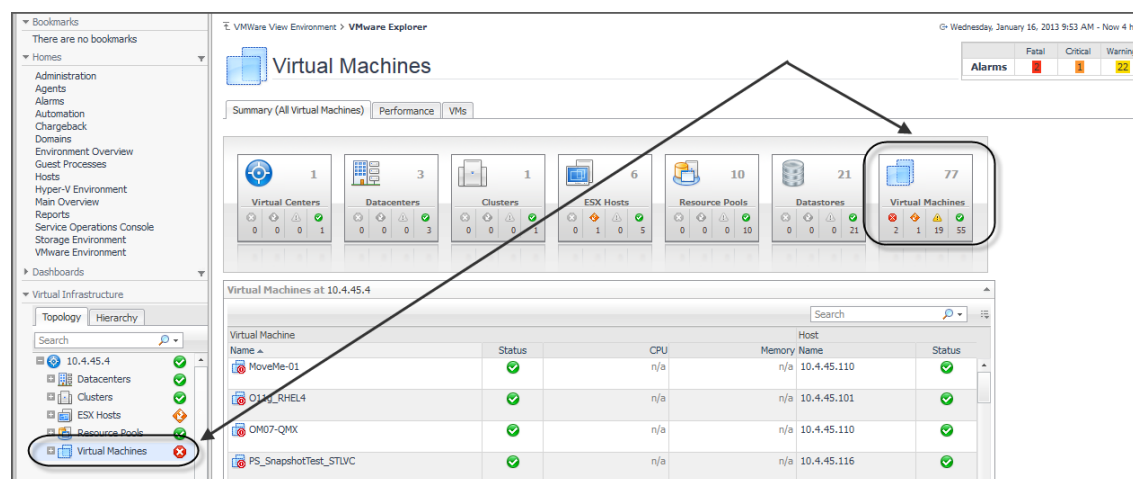
The VMware Explorer dashboard contains the following views: the [Virtual Infrastructure view](#) and [VMware Explorer View](#).

# Virtual Infrastructure view

The **Virtual Infrastructure view** contains a navigation tree on the **Topology** tab that represents the various virtual infrastructure objects: Virtual Centers, Datacenters, Clusters, ESX® Hosts, Resource Pools, and Virtual Machines. For each individual object or group of objects, a status indicator appears, showing the alarm of highest severity that is outstanding for the that object or objects.

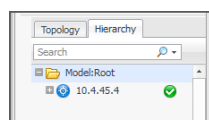
For example, there are 77 virtual machines configured for a VirtualCenter. Fifty-five of the virtual machines have a Normal status, nineteen have a Warning status, one has a Critical status, and another one has a Fatal status. In the Topology view, the virtual machines container for that VirtualCenter displays a Fatal status indicator to show that at least one of the virtual machines associated with the VirtualCenter has an outstanding Fatal alarm.

**Figure 20. Virtual Infrastructure view**



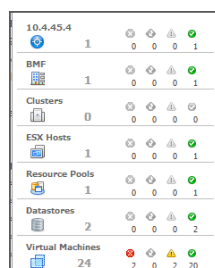
The Hierarchy tab shows the logical layout of VirtualCenter management servers.

**Figure 21. Hierarchy tab**



Hovering over an object in the **Virtual Infrastructure view**, you see a popup that provides a summary of the present state of that object.

**Figure 22. Object state**



Selecting an object or group of objects on either tab of the **Virtual Infrastructure view** displays performance details about your selection in the VMware Explorer. The VMware Explorer takes up the entire display area of the Foglight for Hyper-V browser interface. This view provides significant value to administrators who leverage Foglight for VMware Horizon View to monitor their virtual infrastructure.

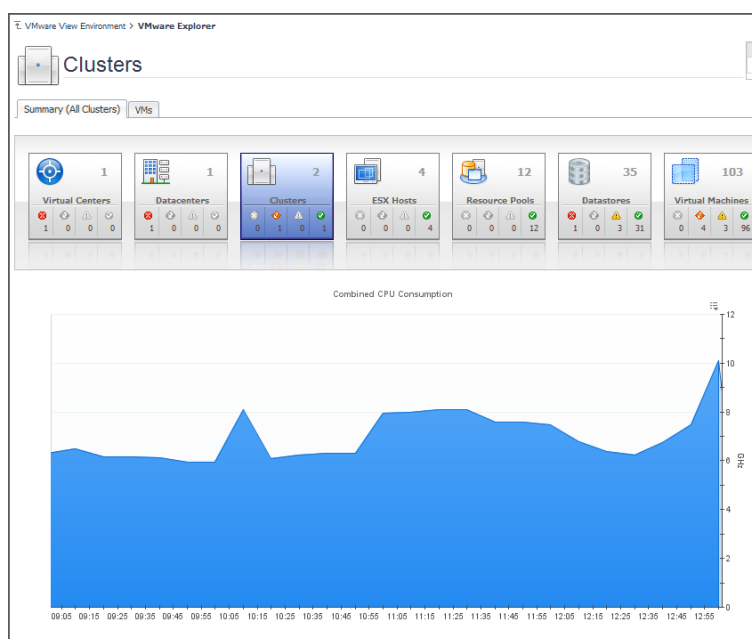
# VMware Explorer View

A set of tiles displayed along the top indicate the type of the selected object or objects, and the related alarm counts.

Additionally, a collection of navigation tabs appears in this view. These navigation tabs vary from object to object, but generally contain a tab to an object summary (typically the default view), a tab to an object performance overview, and one or more tabs to other relevant information.

The display area changes in appearance and content, depending on the selected object or group of objects. For example, if you select an object type container from the Topology view, the Summary tab displays a consumption graph and a table that are representative of the group of objects within that container.

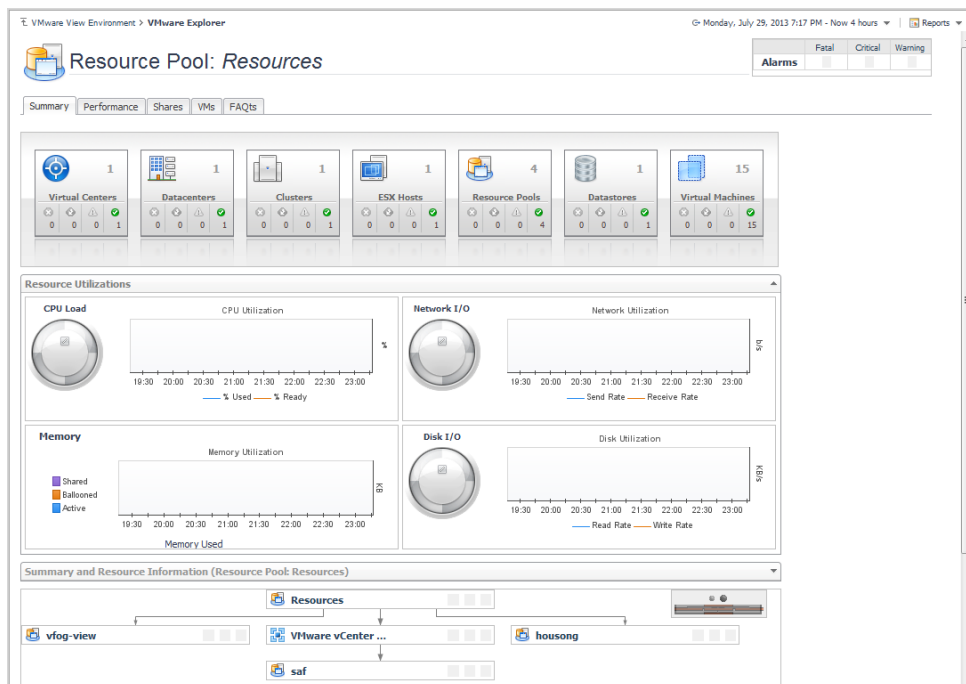
**Figure 23. VMware Explorer View: Clusters**



However, if you select a Resource Pools container, a Resource Pools Relationship Tree is displayed on the Summary tab. This tree contains every resource pool that belongs to the clusters within the associated VirtualCenter. This is useful if you want to see how those resource pools are laid out, or if you want to take a look at the utilization statistics for each configured resource pool on the VirtualCenter.

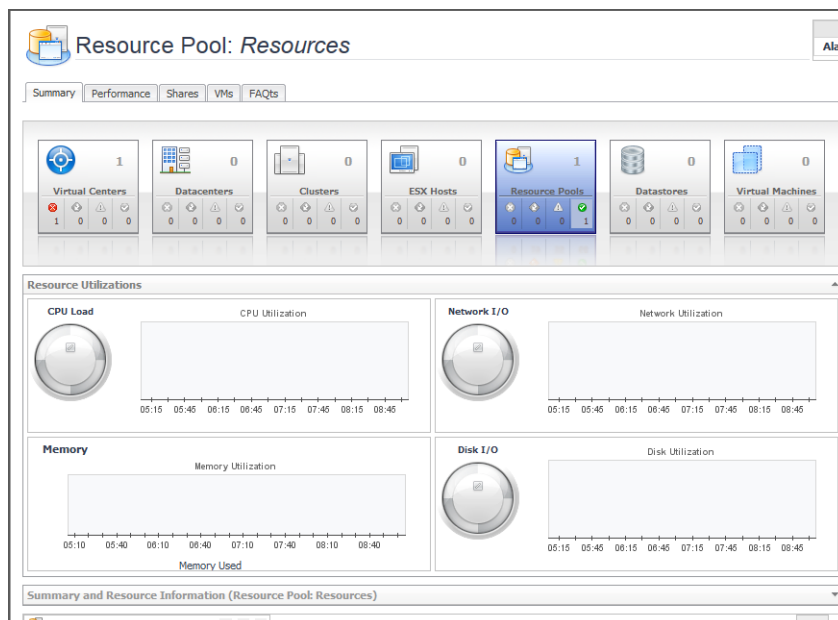


**Figure 24. VMware Explorer View: Resource pool**



Selecting an individual resource pool displays summary and utilization information for that resource pool. This is typically the type of information you see on the Summary tab when you select any individual object from the Virtual Infrastructure view.

**Figure 25. VMware Explorer View: Individual resource pool**



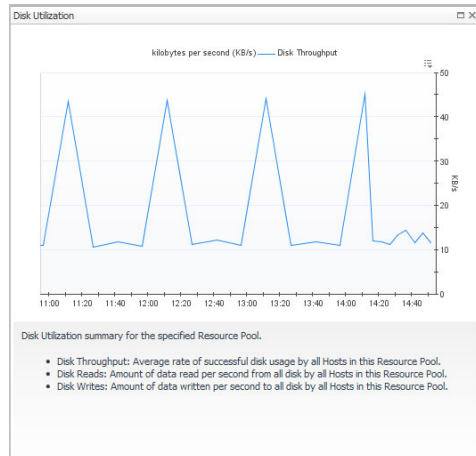
## Utilizations view

The Utilizations view, typically located across the center of the display area tab, provides numerical and graphical representations of utilization metrics associated with the selected object or group of objects. For example,

selecting a single resource pool from the [Virtual Infrastructure view](#) and opening the Performance tab in the display area, displays four graphs in the Utilizations view, showing CPU, memory, disk, and network resource utilizations for the selected resource pool.

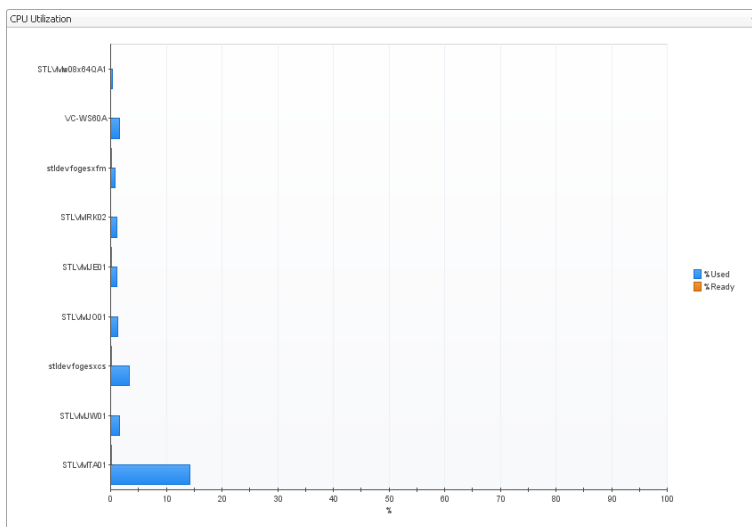
From there, clicking a graph or a spinner shows a larger view of the graph with descriptive text about each metric appearing in the graph.

**Figure 26. Utilizations view: disk utilization**



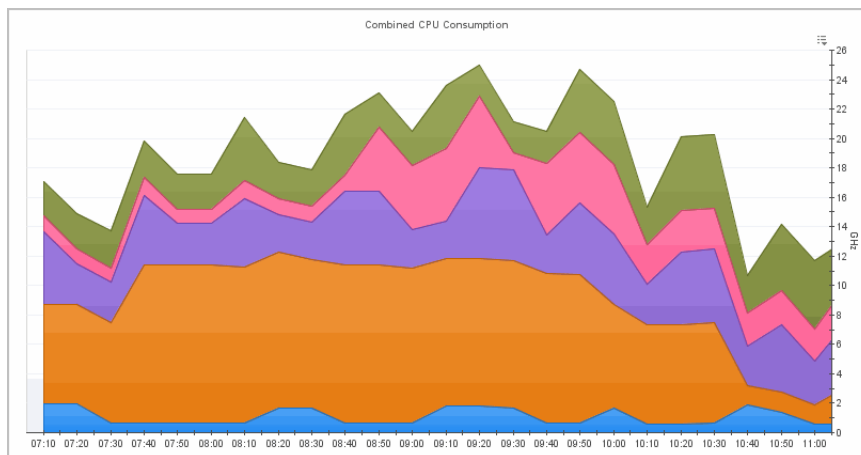
If you open the VMs tab for that same resource pool, the Utilizations view displays one graph illustrating the percent-used and percent-ready CPU utilization for the virtual machines of the resource pool.

**Figure 27. Utilizations view: CPU utilization**



If, however, you select a collection of ESX® Hosts from the [Virtual Infrastructure view](#) and you open the Summary tab, an informative graph appears in place of a Utilizations view. Selecting a collection of objects in the [Virtual Infrastructure view](#) always shows a composite view displaying information about all object instances contained in that collection.

**Figure 28. Utilizations view: Combined CPU consumption**



For reference information on this view, see [Utilizations views](#) on page 76.

## Related Objects views

In addition to the Utilizations view, one or more Related Objects views may appear at the bottom of the display area. These views take the form of tables and list either the parent or child objects or both (whichever are applicable) of the object being viewed, and provide pertinent details about each one. Their appearance depends on the type and range of objects selected in the [Virtual Infrastructure view](#).

For example, if you select a single cluster two Related Objects views appear: one displaying the ESX® hosts that belong to their cluster, and another listing the virtual machines running on those hosts. The views also display the performance metrics associated with each list item.

**Figure 29. Related Objects views for a single cluster**













Server Name	Status	CPU	Memory	NICs	Version	HBAs	Virtual Machines Configured	Running
10.4.45.114	<span style="color: red;">●</span>	8.6 % of 12.8 GHz	67.9 % of 8.0 GB	4	3.0.2	n/a	5	3
10.4.45.112	<span style="color: green;">●</span>	7.6 % of 12.8 GHz	67.0 % of 8.0 GB	4	3.0.2	n/a	5	4

Virtual Machine Name	Status	CPU	Memory	Server Name	Status
stdevfogesxh	<span style="color: orange;">●</span>	11.8 %	7.0 %	10.4.45.114	<span style="color: red;">●</span>
FogW03agent	<span style="color: orange;">●</span>	2.6 %	5.0 %	10.4.45.114	<span style="color: red;">●</span>
W2k_Base	<span style="color: yellow;">●</span>	1.8 %	4.0 %	10.4.45.112	<span style="color: green;">●</span>
Fog511R7M	<span style="color: yellow;">●</span>	6.4 %	17.0 %	10.4.45.112	<span style="color: green;">●</span>
W03_Base	<span style="color: yellow;">●</span>	2.5 %	6.0 %	10.4.45.112	<span style="color: green;">●</span>
FogXPagent	<span style="color: green;">●</span>			10.4.45.112	<span style="color: green;">●</span>
stdevfogesx	<span style="color: green;">●</span>	18.3 %	11.0 %	10.4.45.112	<span style="color: green;">●</span>
FogW03agentKOS	<span style="color: green;">●</span>			10.4.45.114	<span style="color: red;">●</span>
FogW03agentFTR	<span style="color: green;">●</span>			10.4.45.114	<span style="color: red;">●</span>
SttFog42x	<span style="color: green;">●</span>	11.9 %	25.0 %	10.4.45.114	<span style="color: red;">●</span>

However, when you select a cluster container, the **Summary** tab shows a Related Objects view that lists all of the clusters in that container and provides pertinent details about each one.

**Figure 30. Related Objects views for a cluster container**

Cluster at 10.4.45.4						
Key	Name	Status	Resource Pools	Hosts	CPU Used	Memory
	Oracle Database		1	0	 0.0 Hz	 0 %
	PE R610s		19	4	 10.8 GHz	 59 %
	Siebel		1	0	 0.0 Hz	 0 %
	Test :: ( %2f %25 \$ * & ! @ # ^ )		1	0	 0.0 Hz	 0 %

For reference information on this view, see [Related Objects views](#).

## Alarms

The alarm summary in the top-right shows you the number of alarms at each severity level that are outstanding for the selected object. Clicking an alarm count lists the active alarms for the object.

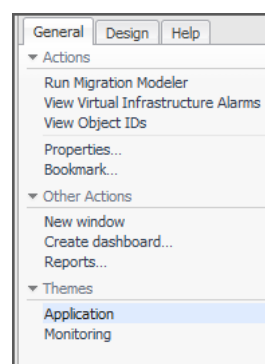
# Accessing VMware® actions and tasks

The action panel operates like a drawer. Its default position is closed. To open the action panel, click the arrow at the far right of the Foglight for Hyper-V browser interface.

The action panel provides you with easy access to a number of useful actions and tasks. However, it only provides additional Foglight for VMware Horizon View related actions when you are viewing the VMware Explorer dashboard.

The following image shows an example of a typical VMware Explorer dashboard action panel.

**Figure 31. VMware Explorer dashboard action panel**



Foglight for VMware Horizon View actions available in the action panel vary depending on the object displayed in the VMware Explorer dashboard.

The following Foglight for VMware Horizon View actions are available from the VMware Explorer dashboard action panel:

- [Run Migration Modeler](#)
- [View Virtual Infrastructure Alarms](#)
- [View Object IDs](#)

## Run Migration Modeler

Under the Actions heading, the Run Migration Modeler link takes you to the VMware Modeler dashboard, which provides you with a mechanism for viewing the impact that migrating a virtual machine will have on a target ESX® Host.

For more information on the Migration Modeler, see the *Managing Virtualized Environments User and Reference Guide*.

## View Virtual Infrastructure Alarms

Under the Actions heading, the View Virtual Infrastructure Alarms link takes you to the VMware Alarms dashboard. For reference information on this dashboard, see [Alarms List view](#).

## View Object IDs

Under the Actions heading, the View Object IDs link takes you to the Object IDs dialog box. The Object IDs dialog box lists all of the objects in the virtual infrastructure with their type and object ID. The object IDs are the true names of the objects. To produce component-specific thresholds, context is required in the form of the relevant object ID.

To narrow down the list of objects, type a relevant text string in the search field, and click **Search**. You can type things like a portion of the object type name (for example, server), a portion of the object name (for example, part of the IP address), or a portion of the object ID. To clear the **Search** box, click **Clear**.

For more advanced search options, click **Advanced**. To narrow down the list to objects of a particular type, type the object type name in the **Type** box. To find the object by name, type the object name in the **Name** box. To find the object by ID, type the object ID in the **Object ID** box.

# Reference

This section contains reference information about views that are included with Foglight for VMware Horizon View. Read this section to find out details about these components: [Views](#).

## Views

Foglight for Hyper-V ships with predefined views to help you monitor your application server environment. This section provides quick reference information about each view.

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

Dashboards are top-level views that do not receive data from other views. Dashboards usually contain a number of lower-level views. The dashboards supplied with Foglight for Hyper-V, as well as those created by users, are available in the navigational panel.

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

Foglight for VMware Horizon View ships with several dashboards that allow you to monitor and configure your virtual environment. Each of these dashboards contains a number of views. This section describes these views in more detail. For more information about the dashboards, see [Interact with Foglight for VMware Horizon View dashboards](#).

Foglight for VMware Horizon View includes the following views:

- [Action panel](#)
- [Administration tab](#)
- [Agents view](#)
- [Alarms List view](#)
- [Cost tab](#)
- [CPU tab](#)
- [Event Analytics tab](#)
- [FAQts view](#)
- [Memory tab](#)
- [Monitor tab](#)
- [Performance tab](#)
- [Processes tab](#)
- [Quick View](#)
- [Related Objects views](#)
- [Resource Pools Relationship Tree view](#)

- [Shares tab](#)
- [Storage tab](#)
- [Summary tab](#)
- [Utilizations views](#)
- [Virtual Environment Overview](#)
- [Virtual Infrastructure view](#)
- [VMware Explorer Primary view](#)
- [VMs tab](#)

## Action panel

The action panel is located at the far right of the Foglight for Hyper-V browser interface.

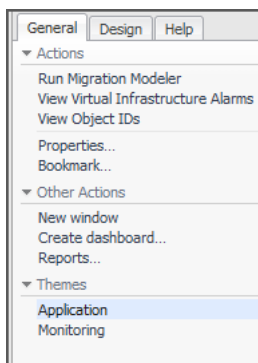
### Purpose and content

The action panel provides you with easy access to a number of useful actions and tasks. However, it only provides additional related actions when you are viewing the VMware Explorer dashboard.

The actions available in the action panel vary depending on the object displayed in the VMware Explorer dashboard.

The following image shows an example of a typical VMware Explorer dashboard action panel.

**Figure 32. VMware Explorer dashboard: action panel**



Under Actions, the action panel may provide the following additional related actions:

- Run Migration Modeler
- View Virtual Infrastructure Alarms
- View Object IDs

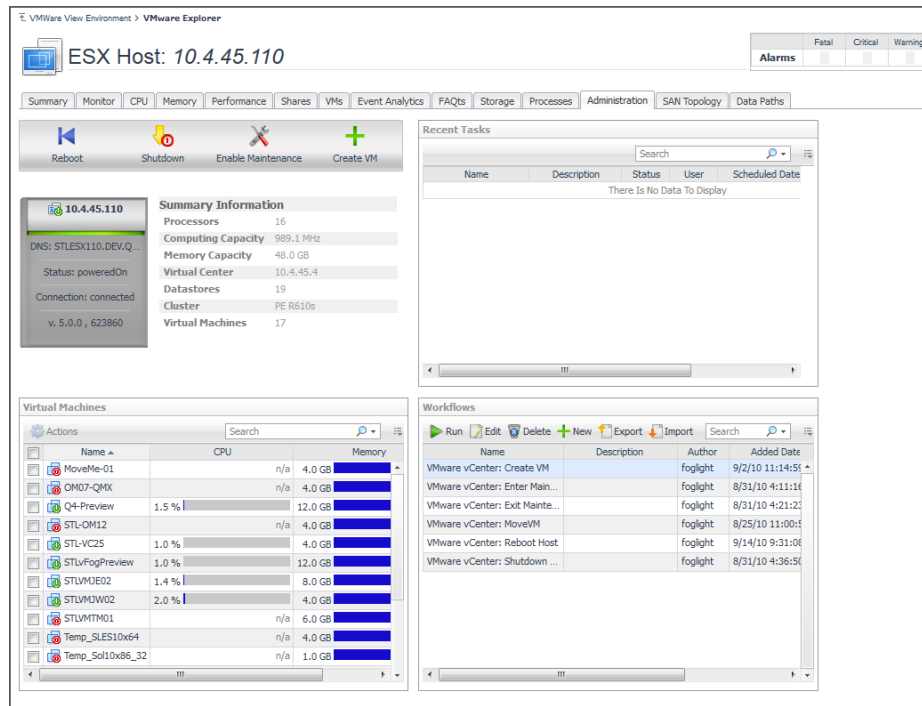
## Administration tab

This tab is available in the VMware Explorer. To find it, open the VMware Explorer and on the [Virtual Infrastructure view](#), that appears on the navigation panel, select an ESX® host or virtual machine instance. In the VMware Explorer, open the **Administration** tab.

## Purpose

The VMware Explorer's **Administration** tab provides access to common administrative tasks. It also shows configuration details for a server or a virtual machine (depending on the selected object type), and some high-level information about the object's resource consumption.

Figure 33. VMware Explorer dashboard: Administration tab



## Description of embedded views

This view is made up of the following embedded views:

- [Recent Tasks](#)
- [ESX Host Configuration](#)
- [ESX Host Summary Information](#)
- [ESX Host Toolbar](#)
- [Snapshots](#)
- [Virtual Machine Configuration](#)
- [Virtual Machines](#)
- [Virtual Machine Summary Information](#)
- [Virtual Machine Toolbar](#)
- [Workflows](#)


## Recent Tasks

This table lists the tasks that are performed for the selected ESX® host or virtual machine. For each task, it shows its description, the date on which the task finished, the task name, the date on which the task is scheduled to run, the task status, and the Foglight user who started the task.




## ESX Host Configuration

Shows physical configuration details for the selected ESX® host.

 | **NOTE:** This view only appears when you are exploring ESX host details.


## ESX Host Summary Information

This view displays additional configuration details for the selected ESX® host. It shows the name of the domain the selected ESX host belongs to, the ESX host's IP address, the total amount of memory, the number of CPUs, the processor type, the length of time the ESX host is running, and the number of virtual machines running on that host.

 | **NOTE:** This view only appears when you are exploring ESX host details.


## ESX Host Toolbar

This toolbar contains buttons for initiating common administrative tasks, such as rebooting and shutting down the ESX® host, enabling its maintenance, and creating virtual machines.

 | **NOTE:** This view only appears when you are exploring ESX host details.


## Snapshots

This view contains a hierarchical view of the selected virtual machine's snapshots. It also contains buttons for initiating common administrative tasks such as creating, deleting, renaming, and reverting to virtual machine snapshots.

 | **NOTE:** This view only appears when you are exploring virtual machine details.


## Virtual Machine Configuration

This view shows the name of the selected virtual machine and its basic configuration, including its status, machine name, configuration, virtualization application (VMware®), and the guest OS.

 | **NOTE:** This view only appears when you are exploring virtual machine details.


## Virtual Machines

This view shows a list of virtual machines associated with the selected ESX® host. For each virtual machine, it displays its name, the total amount of memory that is available to that virtual machine, and the current percentage of time the CPU allocated to the virtual machine executes system code and user programs, including both system and user time.

 | **NOTE:** This view only appears when you are exploring ESX host details.


## Virtual Machine Summary Information

This view shows additional configuration details for the selected virtual machine. For each virtual machine, it displays its IP address, OS name, the number of CPUs and network interface cards used by that virtual machine, the amount of memory and disk storage allocated to the virtual machine, the services associated with the selected virtual machine, and the length of time the virtual machine is running.

 | **NOTE:** This view only appears when you are exploring virtual machine details.

## Virtual Machine Toolbar

This toolbar contains buttons for initiating common administrative tasks, such as powering off the virtual machine, shutting down its guest OS, rebooting, suspending, switching the guest OS to standby mode, deleting, moving, and editing virtual machine configurations.

 | **NOTE:** This view only appears when you are exploring virtual machine details.

## Workflows

This view contains a list of the available workflows along with buttons for creating and editing workflows. A workflow is a collection of tasks that are arranged into a specific order, that you can run multiple times against the same or different set of objects. It provides a way to automate common scenarios and simplify administration in general. For each workflow, this view contains its name and description, the dates on which the workflow was added and updated, and the name of the Foglight user who created the workflow. You can use this view to create, edit, delete, and run workflows, and to import or export them to a file.

**NOTE:** Creating or editing workflows takes you to the Workflow Studio dashboard. This dashboard is defined in the Foglight Cartridge for Automation. For complete details about this dashboard, see the Foglight Automation documentation.

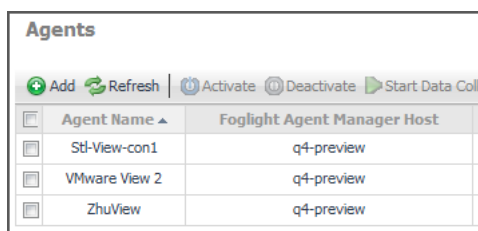
## Agents view

The Agents view appears on the VMware View Environment dashboard. For more information about this dashboard, see [Use the VMware View Environment dashboard](#).

### Purpose and content

The Agents view displays information on the various agent systems that are collecting and sending details to Foglight for VMware Horizon View. This view can be used to verify that agents are properly reporting information at regular intervals to Foglight for VMware Horizon View.

Figure 34. Agents view



Agent Name	Foglight Agent Manager Host
Std-View-con1	q4-preview
VMware View 2	q4-preview
ZhuView	q4-preview

Each agent in the Agents view contains an alarm summary that shows you the number of alarms of each severity that are presently outstanding for the agent.

## Alarms List view

This view is available from the action panel when you click **View Virtual Infrastructure Alarms**. The VMware Alarms dashboard provides an Alarms List view, which takes up the majority of the dashboard.

### Purpose and content

Each alarm row in the Alarms List contains an object icon that identifies the source of the alarm, an alarm icon that indicates the severity of the alarm, the time that the alarm occurred, and the text of the alarm. The columns are sortable so that alarms can be listed in order by source, severity, time or message. Simply click a column heading to sort the table by that column.

Figure 35. Alarms List view

Severity	Time	Rule Name	Alarm Message
	9/28/10 1:39 PM	VMW Datastore Estimated Fill Time	At the present growth rate, Datastore S550_VM300_9 will be full within the next 7 days.
	9/25/10 4:44 PM	VMW Virtual Machine Logical Drive Utilization	Logical drive C:\ on virtual machine stlvm_ora91 has 0.00% available and 100.00% full.
	9/25/10 4:44 PM	VMW Virtual Machine Logical Drive Utilization	Logical drive D:\ on virtual machine stlvm_ora92 has 0.00% available and 100.00% full.
	9/25/10 8:50 PM	VMW Virtual Machine Logical Drive Utilization	Logical drive C:\ on virtual machine STLMMB01 has 0.70% available and 99.30% full.
	9/25/10 10:20 AM	VMW Agent Messages	VirtualCenter Agent::FaultException : Failed to retrieve events data from the collector : Unable to connect to the remote server Make sure the agent collector service is running
	9/29/10 7:39 AM	VMW ESX Server Memory Estimated Fill Time	At the present growth rate Memory resources on Server 10.4.45.116 will be full within the next 30 days.

If you click an alarm's severity icon, a popup for acknowledging or clearing that alarm is displayed. The popup provides a lot of pertinent information about the alarm, such as the rule of origin for the alarm, the history of the alarm, and all of the notes attached to the alarm. If you click the message or any other column in the row, you are provided with a popup menu. From the popup menu, you can choose to view a VMware Explorer dashboard for the corresponding object.

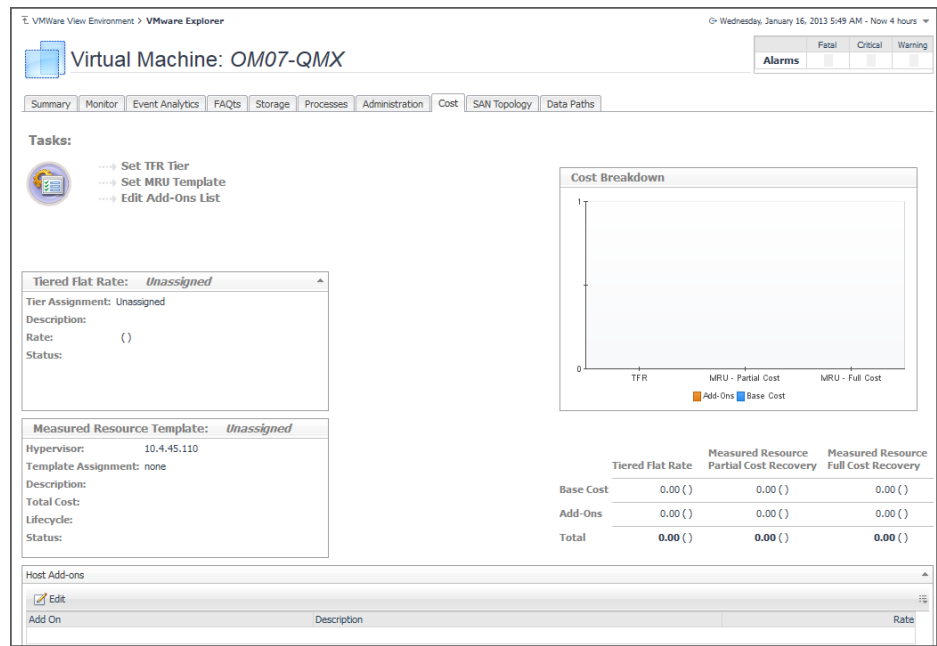
# Cost tab

This tab is available in the VMware Explorer. To find it, open the VMware Explorer and on the [Virtual Infrastructure view](#), that appears on the navigation panel, select a virtual machine instance. In the VMware Explorer, open the **Cost** tab.

## Purpose and content

The VMware Explorer's **Cost** tab contains information about the costs associated with the selected host's usage. The information about these costs is provided by the cost models and host assignments that are configured in Foglight Chargeback. For more information about Foglight Chargeback, see the *Foglight Chargeback User and Reference Guide*.

Figure 36. Cost tab



## Description of embedded views

This view is made up of the following embedded views:

- [Cost Breakdown](#)
- [Host Add-ons](#)
- [Measured Resource Template](#)
- [Tasks](#)
- [Tiered Flat Rate](#)

### Cost Breakdown

This view shows the levels of Tiered Flat Rate (TFR) and Measured Resource Utilization (MRU), including the base cost and the cost of add-ons, if applicable.

### Host Add-ons

This view lists the existing host add-ons. Add-ons are upgrades to any standard host configuration. These upgrades could include hardware, software, licensing, or infrastructure items such as rack space or power backup units. Add-ons consist of other costs incurred in the IT infrastructure.

### Measured Resource Template

This view provides an overview of the measured resource template host assigned to the host. Measured Resource Utilization (MRU) is based on actual percentage utilizations of CPU, Memory, Network, and disk I/O weight. You can create templates based on these levels.

### Tasks

This toolbar contains buttons for initiating wizards that allow you to set up TFR tiers and ESX® host templates, and to edit existing add-ons.

### Tiered Flat Rate

This view provides an overview of the tiered flat rate assignment. A tier is a level of expense for a host machine. Using the Tiered Flat Rates (TFR) you can determine monthly costs of the selected virtual machine.

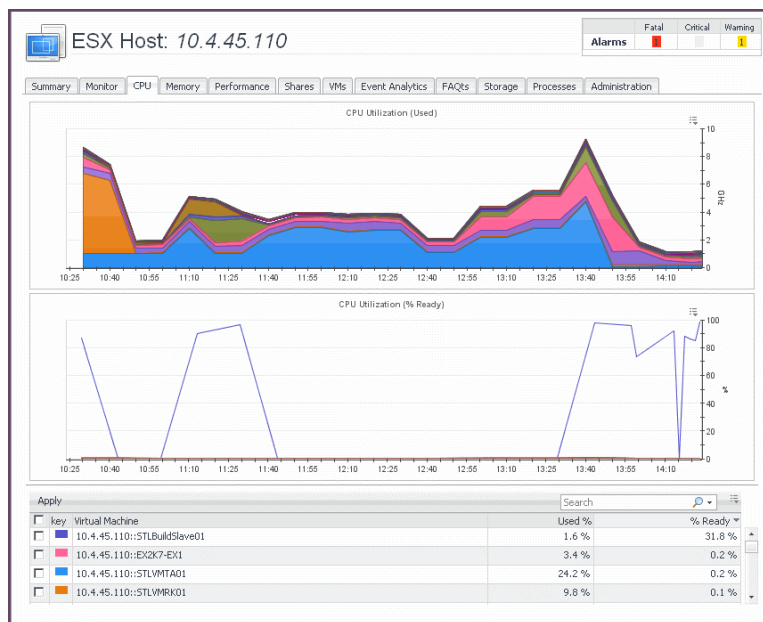
## CPU tab

This tab is available in the VMware Explorer. To find it, open the VMware Explorer and on the [Virtual Infrastructure view](#), that appears on the navigation panel, select an ESX® host instance. In the VMware Explorer, open the **CPU** tab.

### Purpose and content

The VMware Explorer's **CPU** tab displays the combined CPU utilization for an ESX host, showing the amount of processing speeds that are used by each virtual machine that is running on that host. This includes the amount of used processing speed, and the percentage of time the CPU resources are ready for use, all during a selected time period.

Figure 37. CPU tab



## Description of embedded views

This view is made up of the following embedded views:

- [CPU Utilization \(Used\)](#)
- [CPU Utilization \(% Ready\)](#)
- [Virtual Machines](#)

## CPU Utilization (Used)

This view shows the amounts of processing speed used by each virtual machine that is running on the selected ESX host during the selected time period.

## CPU Utilization (% Ready)

This view shows the percentage of time the CPU resources are ready for use by each virtual machine that is running on the selected ESX host during the selected time period.

## Virtual Machines

This view shows a list of all virtual machines that are running on the selected ESX host. For each virtual machine, it shows its name, the percentages of CPU resources that are used and ready for use, along with a color indicator for displaying this information in the [CPU Utilization \(Used\)](#) and [CPU Utilization \(% Ready\)](#) views. It also allows you to show or hide the related resource use from these views.

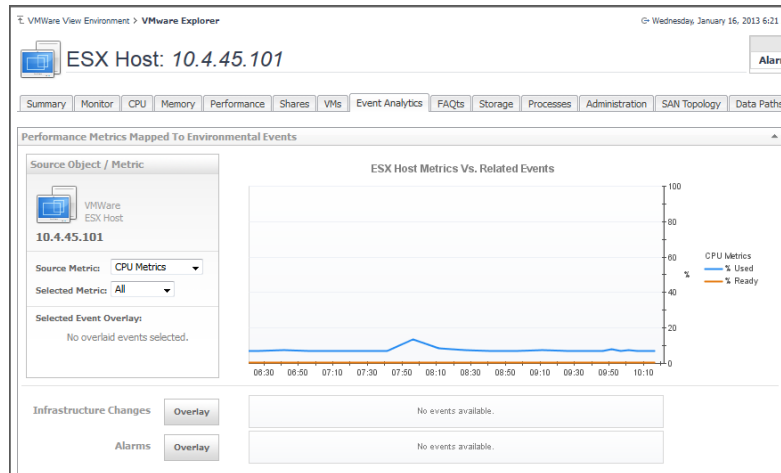
# Event Analytics tab

This tab is available in the VMware Explorer. To find it, open the VMware Explorer and on the [Virtual Infrastructure view](#), that appears on the navigation panel, select an ESX® host or virtual machine instance. In the VMware Explorer, open the **Event Analytics** tab.

## Purpose and content

VMware Explorer's **Event Analytics** tab contains details about the state of resource-related metrics collected about an ESX host or a virtual machine over a selected time period, and also shows any events that occurred during that time frame.

Figure 38. Event Analytics tab



## Description of embedded views

This view is made up of the following embedded views:

- [ESX Host Metrics Vs. Related Events](#)
- [Infrastructure Changes and Alarms](#)
- [Source Object/Metric](#)
- [VM Metrics Vs. Related Events](#)

## ESX Host Metrics Vs. Related Events

This view shows a chart indicating the utilization percentage or all values for one or more metric values selected in the [Source Object/Metric](#) view. If any infrastructure changes occur for the selected server during the selected time period, you can add them as an overlay to the chart using the [Infrastructure Changes and Alarms](#) view. This can give you a good idea on how the current resource consumption affects your environment as a whole. For example, a steady increase in memory consumption can trigger memory utilization alarms, which typically indicates that you need to allocate more memory to the affected ESX Server.

**NOTE:** This view only appears when you are exploring ESX host details.

## Infrastructure Changes and Alarms

This view allows you to add events such as alarms or infrastructure changes as overlays to the [ESX Host Metrics Vs. Related Events](#) or [VM Metrics Vs. Related Events](#) view, and correlate the resource consumption with the stability of your environment.

## Source Object/Metric

This view allows you to select the metrics that appear in the chart view on the right. Possible metric types include: CPU Metrics, Disk Metrics, Memory Metrics, and Network Metrics. For each metric type, you can display the values of a selected metric, or all metric values associated with that type. For example, selecting Disk Metrics gives you an option of displaying Read Rate, Write Rate, or both metrics (All) in the chart. It also indicates if the chart on the right shows any color-coded overlays that represent infrastructure and/or alarm events, in addition to the selected source metric.

## VM Metrics Vs. Related Events

This view shows a chart indicating the utilization percentage or all values for one or more metric values selected in the [Source Object/Metric](#) view. If any infrastructure changes occur for the selected server during the selected time period, you can add them as an overlay to the chart using the [Infrastructure Changes and Alarms](#) view. This can give you a good idea on how the current resource consumption affects your environment as a whole. For example, a steady increase in memory consumption can trigger memory utilization alarms, which typically indicates that you need to allocate more memory to the affected virtual machine.

**NOTE:** This view only appears when you are exploring virtual machine details.

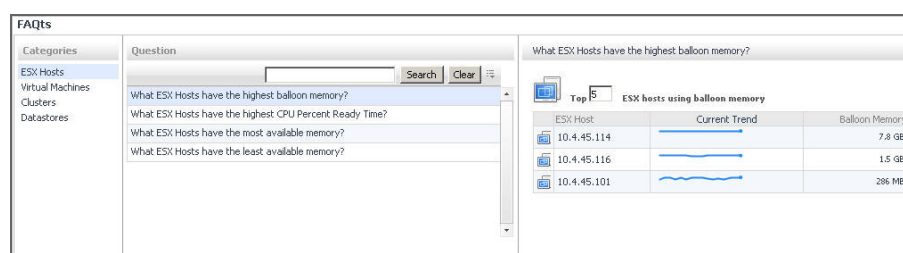
## FAQts view

The FAQts view is provided in the VMware Explorer dashboard and is available in the VMware Explorer Primary view through a navigation tab.

### Purpose and content

Through three embedded views (the Categories, Question, and Answer views), the FAQts view enables you to ask questions and provides the answers to those questions.

Figure 39. FAQts view



### Description of embedded views

The FAQts view is made up of the following embedded views:

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

### Answer

This view provides an answer to the question selected in the [Questions](#) view. The answer appears in the following form:

**Top x** <objects of category>...

where x is the number of objects of the category you provided in the [Categories](#) view.

Specify x by entering a number. The answer is relative to the subset of the infrastructure you are viewing in the dashboard. For example, the top 5 datastores are different for each individual cluster in the infrastructure.

### Categories

This view lists the categories for which questions can be answered for you by Foglight for Hyper-V.

Click a category in the list to select it.

## Questions

This view lists the questions, for the category selected in the [Categories](#), that can be answered for you by Foglight for Hyper-V.

Click a question in the list to select it.

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

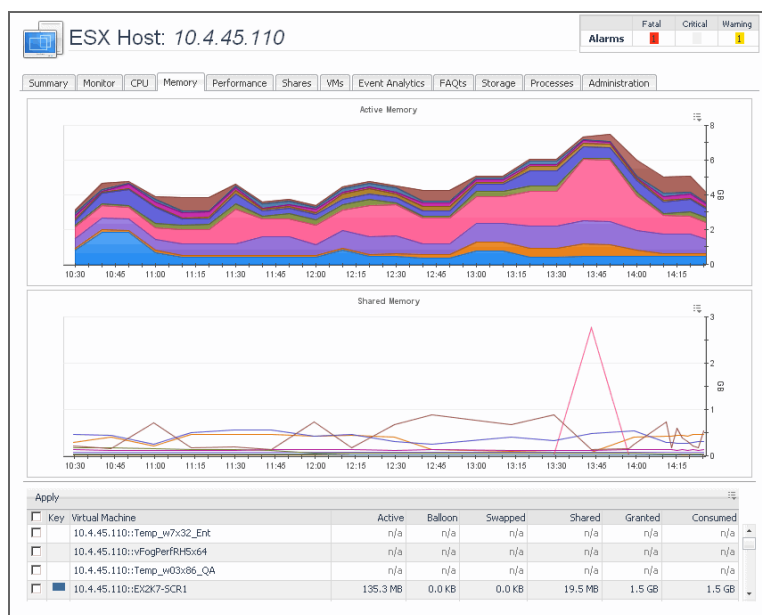
## Memory tab

This tab is available in the VMware Explorer. To find it, open the VMware Explorer and on the [Virtual Infrastructure view](#), that appears on the navigation panel, select an ESX® host instance. In the VMware Explorer, open the **Memory** tab.

### Purpose and content

The VMware Explorer's **Memory** tab displays the combined memory utilization for an ESX host, showing the amount memory used by each virtual machine that is running on that host. This includes the amount of active and shared memory in GB, all during a selected time period.

Figure 40. Memory tab



### Description of embedded views

This view is made up of the following embedded views:

- [Active Memory](#)
- [Shared Memory](#)
- [Virtual Machines](#)

### Active Memory

This view shows the amounts of active memory used by each virtual machine that is running on the ESX host during the selected time period.



## Shared Memory

This view shows the amounts of shared memory used by each virtual machine that is running on the ESX host during the selected time period.

## Virtual Machines

This view shows a list of all virtual machines that are running on the selected ESX host. For each virtual machine, it shows its name along with a color indicator for displaying this information in the [Active Memory](#) and [Shared Memory](#) views. This allows you to show or hide the related resource use from these views.

The list also shows the following information for each virtual machine:

- **Active.** Amount of physical memory that is actively being used.
- **Balloon.** Amount of memory being used by the VMware® Memory Control Driver to allow the virtual machine OS to selectively swap memory.
- **Consumed.** Amount of memory that is consumed by current processes.
- **Granted.** Total amount of memory that is allocated to the virtual machine.
- **Shared.** Amount of memory that is freed up on the host due to transparent page sharing.
- **Swapped.** Amount of memory that is stored in disk swap space.

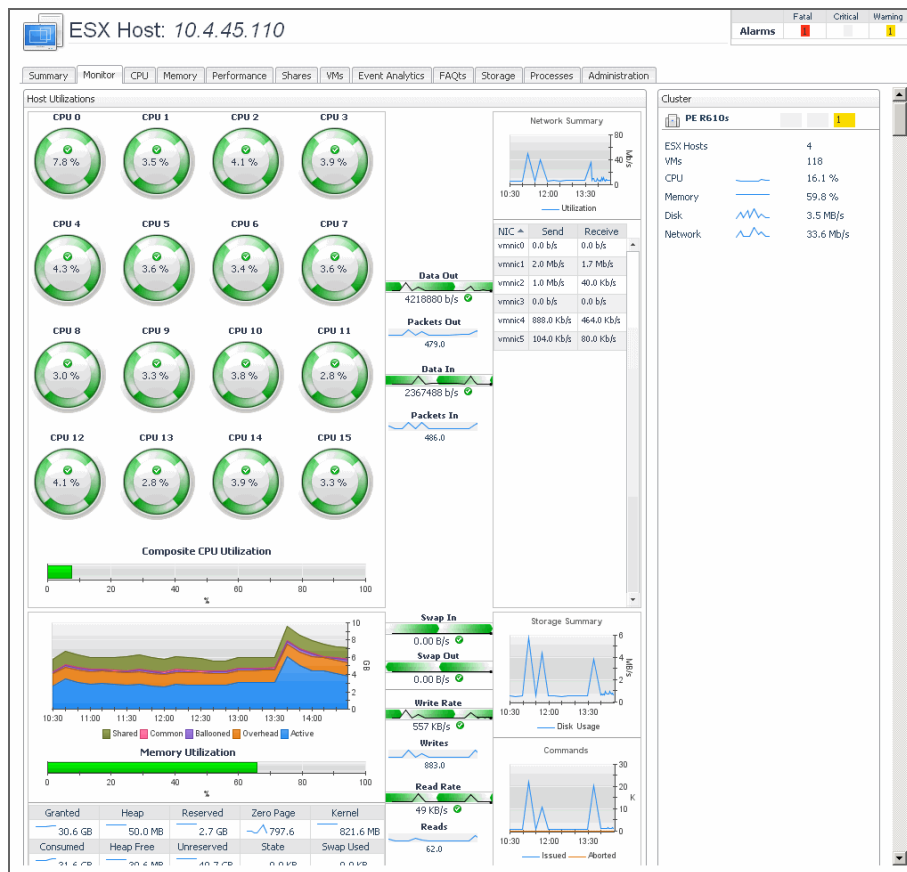
## Monitor tab

This tab is available in the VMware Explorer. To find it, open the VMware Explorer and on the [Virtual Infrastructure view](#), that appears on the navigation panel, select the server or virtual machine instance. In the VMware Explorer, open the **Monitor** tab.

### Purpose

The VMware Explorer's **Monitor** tab shows details of system resources consumption for a server or a virtual machine.

Figure 41. Monitor tab



## Description of embedded views

This view is made up of the following embedded views:


- [Cluster](#)
- [Datacenter](#)
- [Host Utilizations](#)
- [Resource Pool](#)
- [ESX Host](#)
- [Virtual Machine Utilizations](#)
- [Virtual Machines](#)
- [Virtual Machine Messages](#)

## Cluster

This view shows the numbers of ESX® hosts and virtual machines the selected ESX host or virtual machine belongs to. It also shows the cluster's combined current CPU and memory utilization along with the disk and network I/O rates, and any alarm counts associated with the cluster, broken by the alarm state.


## Datacenter

This view shows the number of ESX hosts and virtual machines in the datacenter the selected virtual machine is associated with. It also shows the datacenter's combined current CPU and memory utilization along with the disk and network I/O rates, and any alarm counts associated with the datacenter, broken by the alarm state.

 | **NOTE:** This data only appears when exploring virtual machine details.


## Host Utilizations

This view shows the utilization of the selected server's resources. It shows the current CPU utilization for each CPU, and the composite CPU utilization across all CPUs on the selected ESX host. This view also provides insights into memory usage, and disk and network IO rates.

 | **NOTE:** This data only appears when exploring ESX host details.


## Resource Pool

This view shows the numbers of virtual machines in the resource pool the selected virtual machine is associated with. It also shows the resource pool's combined current CPU and memory utilization along with the disk and network I/O rates, and any alarm counts associated with the resource pool, broken by the alarm state.

 | **NOTE:** This data only appears when exploring virtual machine details.


## ESX Host

This view shows the numbers of virtual machines that are running in the ESX Host to which the selected virtual machine belongs. It also shows the ESX Host's combined current CPU and memory utilization along with the disk and network I/O rates, and any alarm counts associated with the virtual machines, broken by the alarm state.

 | **NOTE:** This data only appears when exploring virtual machine details.


## Virtual Machine Utilizations

This view shows the utilization of the resources allocated to the selected virtual machine. It shows the current CPU utilization for each allocated CPU, and the composite CPU utilization across all CPUs on the selected ESX host. This view also provides insights into memory usage, and disk and network IO rates.

 | **NOTE:** This data only appears when exploring virtual machine details.


## Virtual Machines

This view shows a list of virtual machines associated with the selected ESX host. For each virtual machine, the list shows its name, followed by the total counts of alarms associated with that VM, broken down by alarm types (normal, warning, critical, fatal). This view also indicates how many virtual machines are currently running.

 | **NOTE:** This data only appears when exploring ESX host details.

## Virtual Machine Messages

This view shows a list of messages associated with the selected virtual machine.

 | **NOTE:** This data only appears when exploring virtual machine details.

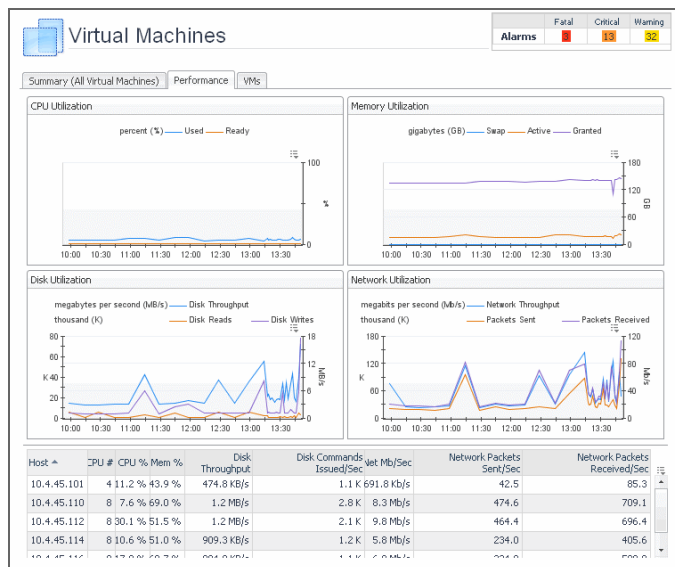
# Performance tab

This tab is available in the VMware Explorer. To find it, open the VMware Explorer and on the [Virtual Infrastructure view](#), that appears on the navigation panel, select a Virtual Center, datacenter, cluster, ESX® host, resource pool, or one of the following containers: Datacenters, ESX Hosts, Resource Pools, or Virtual Machines. In the VMware Explorer, open the **Performance** tab.

## Purpose and content

This tab displays the resource utilization for the selected object or group of objects over a selected period of time.

Figure 42. Performance tab



## Description of embedded views

This tab is made up of the following embedded views:

- [CPU Utilization](#)
- [Disk Utilization](#)
- [Hosts](#)
- [Memory Utilization](#)
- [Network Utilization](#)

### CPU Utilization

This view shows the CPU utilization summary for the selected component based on its total capacity, including the percentage of available CPU processing that is currently used, and the percentage of time the CPU is ready but is not used due to other reasons, during a selected time period.

### Disk Utilization

This view shows the disk utilization summary for the selected component, including the disk throughput rate, and the rates of data that is read from or written to the disk, during a selected time period.

### Hosts

This view shows a list of all ESX hosts associated with the selected component. For each host, it shows its name, the number of CPUs, the current percentages of CPU and memory use, disk throughput rate, rate at which disk commands are issued, and the rate at which data packets are sent to and received from the network.

**NOTE:** This view only appears when you are exploring virtual centers, Datacenters container, datacenters, ESX Host container, Resource Pools container, resource pools, or Virtual Machines container.

## Memory Utilization

This view shows the physical memory utilization summary for the selected component, broken into the amounts of memory that is swapped to disk, actively used, and allocated, all during a selected time period.

## Network Utilization

This view shows the network utilization summary for the selected component, including the average rate of network throughput, and the amounts of data sent to and received from the network.

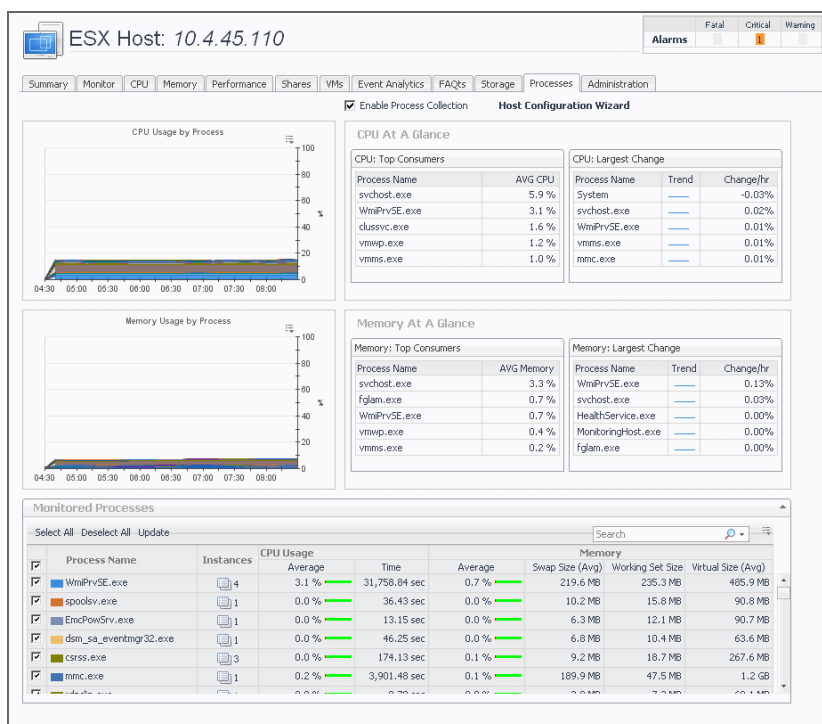
# Processes tab

This tab is available in the VMware Explorer. To find it, open the VMware Explorer and on the [Virtual Infrastructure view](#), that appears on the navigation panel, select a Virtual Center, ESX® host, or virtual machine instance. In the VMware Explorer, open the **Processes** tab.

## Purpose and content

This tab only appears when you are exploring individual Virtual Centers, ESX hosts, and virtual machines, and have the Cartridge for Guest Processes Investigation installed and active. It displays an organized view of process information gathered by the Cartridge for Guest Process Investigation from the virtual or physical machine configured to send process information. When you open this tab, the process information for the selected server or virtual machine appears, allowing you to view the current CPU, memory, and monitored process statistics.

Figure 43. Processes tab



For complete information about the views that appear on this tab, see the *Investigating Guest Processes User and Reference Guide*.

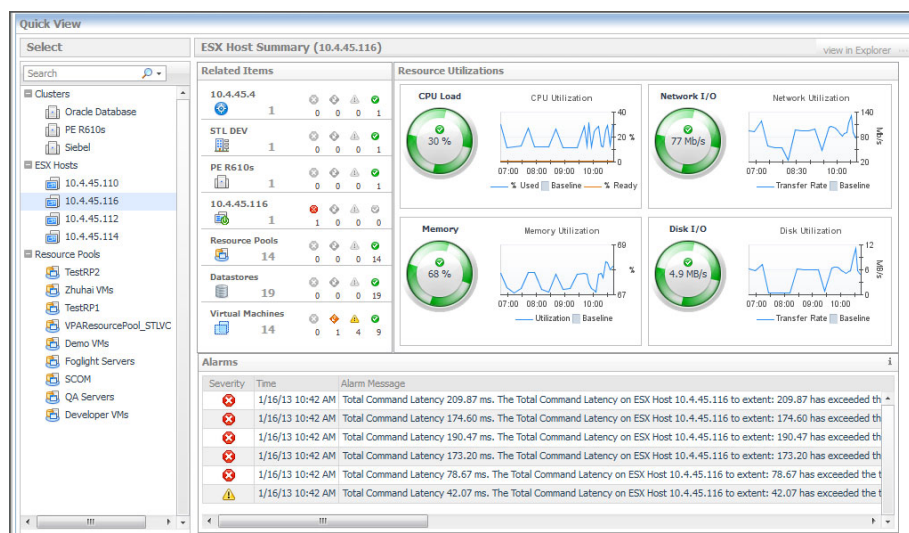
# Quick View

The Quick View appears in the middle of the VMware View Environment dashboard. For more information about this dashboard, see [Use the VMware View Environment dashboard](#).

## Purpose and content

The Quick View displays summary information about the objects you select from the VMware View Environment Details tab.

Figure 44. Quick View



The Quick View is made up of two embedded views: the Object Tree view and the Object Summary view. Depending on what is displayed in the Object Tree view, the Object Summary view, located at the right of the Quick View, displays summary information for either a single object or for a group of objects of a particular type.

## Description of embedded views

The Quick-View is made up of the following embedded views:

- [Object Tree](#)
- [Object Summary](#)

## Object Tree

The Object Tree view is located at the left of the Quick View and displays objects based on what is selected on the tiles of the VMware View Environment dashboard.

Depending on what is displayed in the Object Tree view, the Object Summary view displays summary information for either a single object or for a group of objects of a particular type.

If the Object Tree view is displaying a list of objects of a particular type, you can click an object in the list to have the Object Summary view display summary information for that object.

## Object Summary

The Object Summary view is located at the right of the Quick View and displays summary information for a single object or for a list of objects, depending on what is displayed in the Object Tree view.

The Object Summary view can display a number of embedded views (such as a Top Consumer view, an Inventory view, a Resource Utilizations view, and an Alarms view). The views the Object Summary view displays depend on the object or list of objects for which the Object Summary view is providing information.

When viewing information about a single object, the Object Summary view consists of an Inventory view and a Resource Utilizations view.

The Inventory view shows all of the objects related to the object selected in the Object Tree view, along with their respective alarm state counts. All objects in the object relationship hierarchy, including the selected object, are shown in the Inventory view, so that you see the entire relationship hierarchy for the selected object. Each level in the hierarchy is labelled with the corresponding object type name. When there is only one object at a particular level in the hierarchy, the object name is displayed instead of the object type name.

When the Inventory view shows multiple objects for a particular object type, you can click the object type icon, the object type name, or the object count to view a popup that displays a complete list of the objects, along with their respective states.

## Related Objects views




At least one Related Objects view is provided in the VMware Explorer dashboard.

Related Objects views are part of the VMware Explorer Primary view and are typically located at the bottom of the Primary view. More than one Related Objects view may appear at a time.




### Purpose and content

Related Objects views provide summary information on either the parent or child objects or both (whichever is applicable) of the object being viewed in the dashboard.

**Figure 45. Related Objects views**

ESX Hosts at PE R610s						
ESX Host						
Host Name ▲	Status	CPU	Memory	NICs	Version	HBAs
 10.4.45.110	✓	10.2 % of 42.6 GHz	71.2 % of 48.0 GB	6	5.0.0	4
 10.4.45.112	✓	14.3 % of 42.6 GHz	70.1 % of 48.0 GB	6	5.0.0	4
 10.4.45.114	✓	11.0 % of 42.6 GHz	54.7 % of 48.0 GB	6	5.0.0	4

Virtual Machines at PE R610s						
Virtual Machine						
Name ▲	Status	CPU	Memory	Name	Host	
 MoveMe-01	✓	n/a	n/a		10.4.45.110	
 OM07-QMX	✓	n/a	n/a		10.4.45.110	
 PS_SnapshotTest_STLVC	✓	n/a	n/a		10.4.45.116	

Related Objects views differ from each other and may not appear at all depending on the object or collection of objects selected from the Virtual Infrastructure view and on the navigation tab selected from the VMware Explorer Primary view heading.

Related Objects views for an individual object display tables that list either the parents or descendents or both (whichever is applicable) of the selected object and provide pertinent summary details about each one. The Related Objects view for a collection of objects displays a table that lists all of the objects in the selected collection and provides pertinent summary details about each one. You can sort Related Objects view tables by a particular column by clicking the corresponding column heading. If you select an object from the table by clicking on one of the table rows, all of the views in the VMware Explorer dashboard get updated with information about that object.

## Resource Pools Relationship Tree view

The Resource Pools Relationship Tree view is provided in the VMware Explorer dashboard. If you select a Resource Pool container from the Topology view on the Virtual Infrastructure view and click the Summary

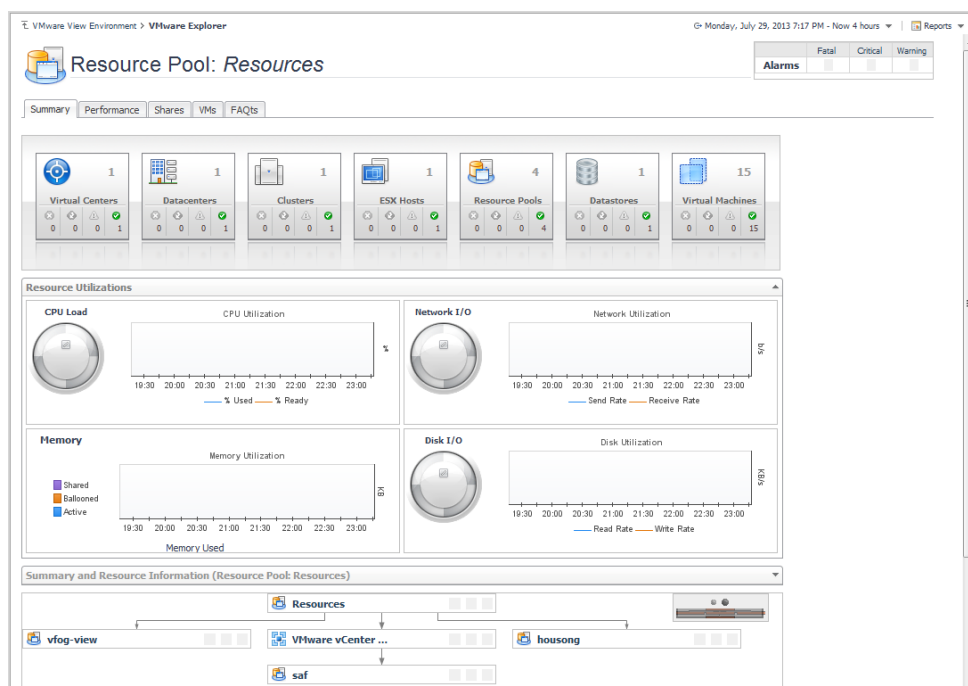
navigation tab within the VMware Explorer Primary view, a Resource Pools Relationship Tree view is displayed in the Primary view. A Resource Pools Relationship Tree contains every resource pool that belongs to the clusters within the associated VirtualCenter.

For more information about the VMware Explorer dashboard, see [VMware Explorer View](#) on page 48.

## Purpose and content

The Resource Pools Relationship Tree view is useful if you want to see how the resource pools within the clusters are laid out or if you want to take a look at the utilization statistics for each configured resource pool on the VirtualCenter.

**Figure 46. Resource Pools Relationship Tree view**



The default Resource Pools Relationship Tree simply displays the names of the various resource pools and their parent/child relationships.

You can use the Normal Zoom Level button on the mini map at the top right of the Relationship Tree to zoom into a more detailed version of the Tree. You can use the Minimized Zoom Level button on the mini map to zoom back out again.

You can browse through a Relationship Tree by clicking and dragging the rectangular shadow provided on the mini map.

## Shares tab

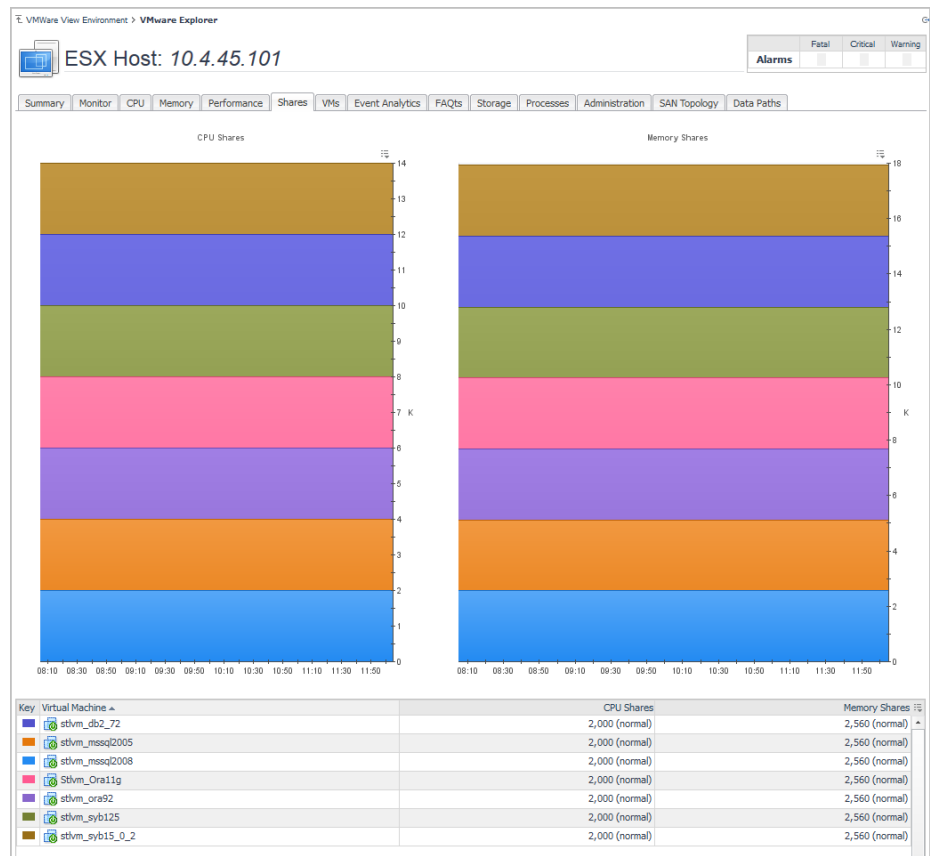
This tab is available in the VMware Explorer. To find it, open the VMware Explorer and on the [Virtual Infrastructure view](#), that appears on the navigation panel, select a cluster, ESX® host, or resource pool instance. In the VMware Explorer, open the **Shares** tab.

## Purpose and content

The VMware Explorer's **Shares** tab displays the CPU and memory shares that are in use by the virtual machines associated with the selected component.



Figure 47. Shares tab



## Description of embedded views

This view is made up of the following embedded views:

- [CPU Shares](#)
- [Memory Shares](#)
- [Virtual Machines](#)

## CPU Shares

This view shows the CPU shares that are in use by the virtual machines associated with the selected cluster, ESX host, or resource pool instance.

## Memory Shares

This view shows the memory shares that are in use by the virtual machines associated with the selected cluster, ESX host, or resource pool instance.

## Virtual Machines

This view shows a list of all virtual machines that are associated with the selected cluster, ESX host, or resource pool instance. For each virtual machine, it displays its name along with a color indicator for displaying this information in the [Active Memory](#) and [Shared Memory](#) views. The list also shows the numbers of CPU and memory shares used by each virtual machine.

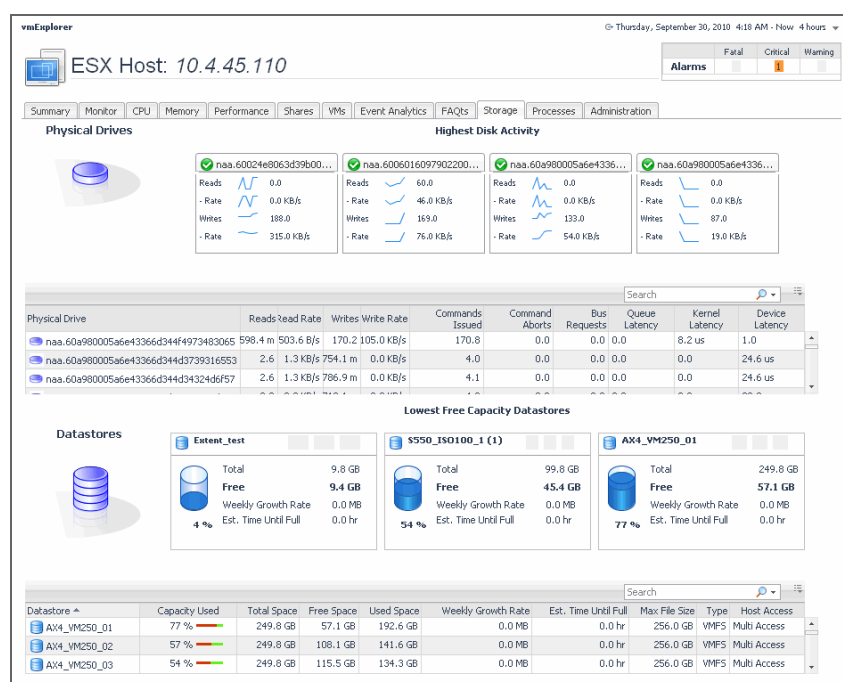
# Storage tab

This tab is available in the VMware Explorer. To find it, open the VMware Explorer and on the [Virtual Infrastructure view](#), that appears on the navigation panel, select a Virtual Center, Datacenter, Cluster, ESX® host, or virtual machine instance. In the VMware Explorer, open the **Storage** tab.

## Purpose and content

The VMware Explorer **Storage** tab displays combination of embedded views organized into physical drive and logical disk sections. It identifies the physical drives with the highest disk activity, and the logical drives with the lowest capacity. It also lists all physical drives for the selected server, their read and write rates, along with the logical drives, the space used on each and shows data growth patterns and the related estimates.

Figure 48. Storage tab



## Description of embedded views

This view is made up of the following embedded views:

- [Datastores](#)
- [Logical Disks](#)
- [Physical Drives](#)

## Datastores

This view contains information about the used, free, and total space of the selected components's datastores, along with projected short-term estimates, given the current growth patterns. It also identifies the datastores that have the lowest percentage of free space. For each identified datastore, it shows the total amount of datastore space, including used and free space, free space, weekly growth rate, the current percentage of the used disk space, and the estimated time after which the datastore will be full.

## Logical Disks

This view contains information about the used, free, and total space of the selected virtual machine's logical disks, along with projected short-term estimates, given the current growth patterns. It also identifies the logical disks that

have the lowest percentage of free disk space. For each identified disk, it shows the total amount of disk space, including used and free space, free disk space, weekly growth rate, the current percentage of the used disk space, and the estimated time after which the disk will be full.

**i | NOTE:** This view only appears when you are viewing virtual machine details.

## Physical Drives

This view contains information about the read and write activities that take place on the physical drives of the selected component. It identifies the physical drives that have the highest amount of disk activity. For each identified drive, it shows the number of reads and writes, along with their read and write rates. It also contains a list of all physical drives that shows the numbers of read and write requests, and the rate at which the data is read from to or written to the selected drive, all during a selected time period.

**i | NOTE:** This view only appears when you are viewing virtual machine or ESX host details.

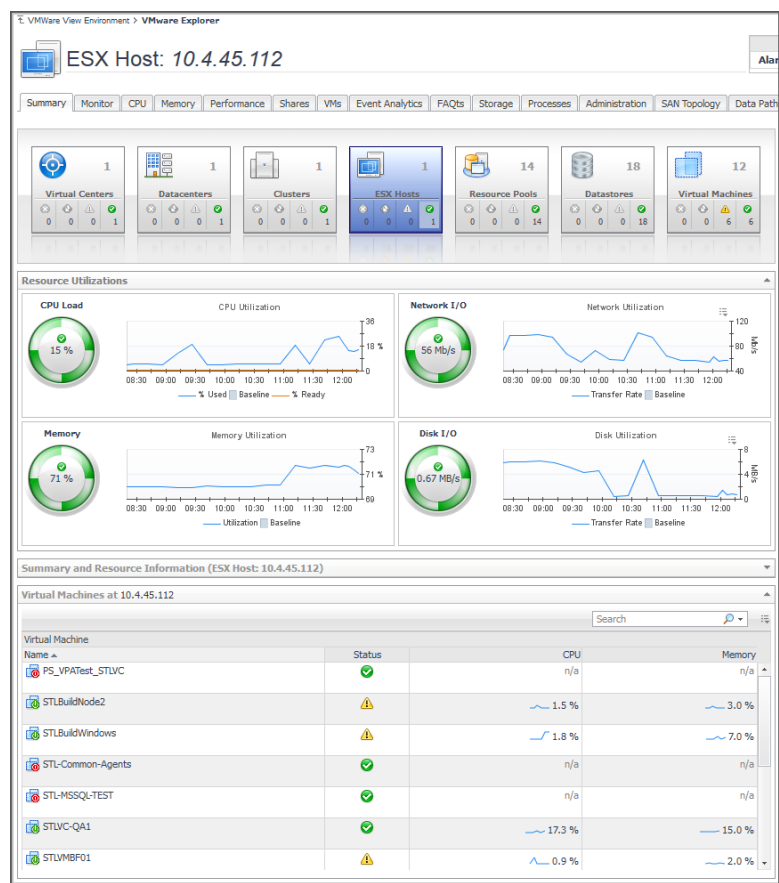
## Summary tab

The Summary tab is provided as part of the VMware Explorer dashboard Primary view. You can open this tab from the top of the [VMware Explorer Primary view](#). For more information about the VMware Explorer dashboard, see [Use the VMware Explorer](#) on page 46.

### Purpose and content

The Summary tab provides a hierarchical inventory, in the form of tiles, of the objects that are related to the object or group of objects selected.

Figure 49. Summary tab



Each tile shows how many of the corresponding object type there are, as well as the count of objects of that type in each of the alarm states (normal, warning, critical, fatal).

More detailed information for the selected object or objects is displayed in the collapsible views below the Summary tab.

On a tile, click the object type icon, the object type name, or the object count, to view a popup that lists all objects of the corresponding type, along with their respective states. Click a column header on the popup to change the sort order. Click an object in the popup list to view details for that object in the VMware Explorer dashboard.

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

If an alarm state has a count of zero, then you can not select that alarm state. When you click a normal state icon or count, the VMware Explorer page is refreshed, but you do not see an alarms popup because there are no alarms associated with the normal state.

## Utilizations views

A Utilizations view is provided in the VMware Explorer dashboard. The Utilizations view is part of the [VMware Explorer Primary view](#) and is typically located at the center of the Primary view. For more information about the VMware Explorer dashboard, see [Use the VMware Explorer](#) on page 46.

### Purpose and content

The Utilizations view provides numerical and graphical representations of utilization metrics associated with the single object (datacenter, cluster, ESX® Server, resource pool, or virtual machine) or collection of objects of a particular type (datacenters, clusters, ESX Servers, resource pools, or virtual machines) that is selected.

The metrics and the amount of detail displayed on the Utilizations view vary depending on the type of object that is being viewed.

A Utilizations view may not appear at all depending on the object or collection of objects selected from the Virtual Infrastructure view and on the navigation tab selected from the VMware Explorer Primary view heading.

Within a single object Utilizations view, you can hover the cursor over any metric to see a description of that metric, and you can click any metric or chart to see a popup with a detailed chart.

Within a collection of objects Utilizations view, you can hover the cursor over any graph to see an exact unit measurement that corresponds to the placement of the cursor, and you can click any metric or chart to see a popup with a detailed chart.

## Single Object Utilizations views

When you select a single object (datacenter, cluster, ESX Server, resource pool, or virtual machine) from the Virtual Infrastructure view, summary information and a Utilizations view is displayed under the Summary tab in the Primary view. Both the metrics and the amount of detail displayed vary depending on the type of object you select.

Under the Summary tab, a typical Utilizations view for an individual object provides detailed information on the four core ESX infrastructure resources: CPU, memory, disk usage, and network usage. Under other navigation tabs, the Utilizations view for an individual object provides different information. For example, under the VMs tab for an ESX Host, the Utilizations view displays a graph illustrating the percent-used and percent-ready CPU utilization for the virtual machines of that ESX Host. Under still other navigation tabs, like the Memory tab for an ESX Host, the Utilizations view is replaced with other pertinent information.

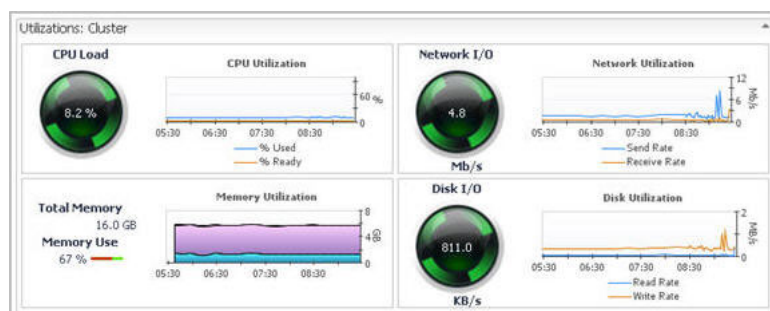
**i** | **NOTE:** If the utilizations view is presenting metrics using spinners, the color of a spinner reflects the alarm state of the object with respect to the metric the spinner is presenting.

Within a single object Utilizations view, you can hover the cursor over any metric to see a description of that metric, and you can click any metric or chart to see a popup with a detailed chart.

In a Utilizations view that contains alarm severity level details, you can click an alarm status indicator to see the fatal, critical, and warning alarms for the associated object.

The following image shows a Utilizations view for a cluster object. As explained above, you can hover the cursor over any metric in a Utilizations view to see a description of the metric, and you can click any metric or chart to see a popup with a detailed chart. For example, if you click the CPU Load gauge for a cluster object, a graph of CPU utilization over the time range specified for the VMware Explorer dashboard is displayed. If you click the Memory Utilization graph, a larger view of the graph with descriptive text about each memory metric is displayed.

**Figure 50. Utilizations view for a cluster object**



## Object Collection Utilizations views

When a collection of objects of a particular type (datacenters, clusters, ESX Servers, resource pools, or virtual machines) is selected from the Virtual Infrastructure view, summary text and a chart—or other compositional information for the collection—are displayed under the Summary tab in the Primary view. No Utilizations view is displayed.

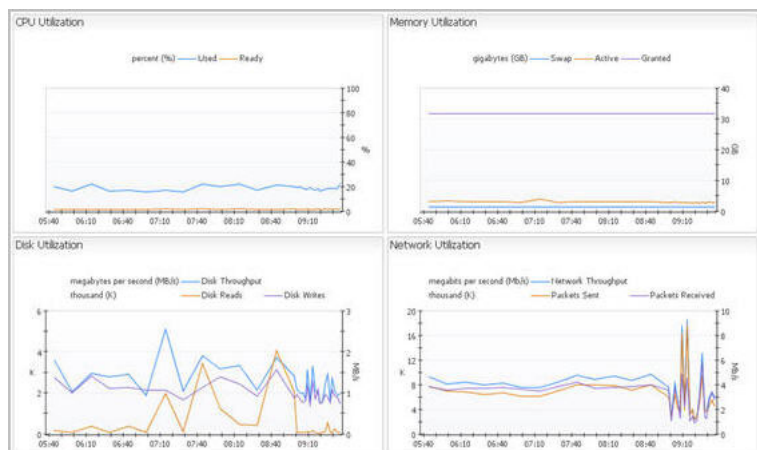
Under some of the other navigation tabs (the Performance and VMs tabs, for examples) in the Primary view, the Utilizations view does appear for collections of objects. Under the Performance tab, the Utilizations view typically displays four graphs showing CPU, memory, disk, and network resource utilizations for the objects in the selected

collection. Under the VMs tab, the Utilizations view typically displays a graph illustrating the percent-used and percent-ready CPU utilization for the virtual machines of the selected collection.

Within a collection of objects Utilizations view, you can hover the cursor over any graph to see an exact unit measurement that corresponds to the placement of the cursor, and you can click any metric or chart to see a popup with a detailed chart.

The following image shows a Utilizations view for a collection of ESX Server objects.

**Figure 51. Utilizations view for a collection of ESX Server objects**



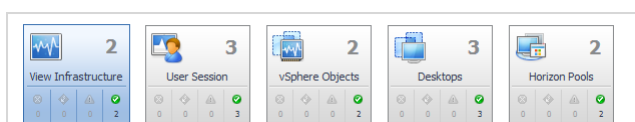
## Virtual Environment Overview

Virtual Environment Summary dashboard provides a Virtual Environment Overview. The Virtual Environment Overview is located at the top of the dashboard. For more information about this dashboard, see [Use the VMware View Environment dashboard](#).

### Purpose and content

The Virtual Environment Overview provides you with an overview of the selected virtual environment.

**Figure 52. Virtual Environment Overview: tiles**



The overview has a tile for each type of object in your virtual infrastructure. Each tile shows how many of the corresponding object type there are in your virtual infrastructure, as well as the count of objects of that type in each of the alarm states (normal, warning, critical, fatal).

Click the object type icon, the object type name, or the object count, to view summary information for that entire object type in the Quick-View. Click an alarm state (for example, warning) on a tile to view summary information in the Quick-View for the objects of that type that are in the selected alarm state.

If an alarm state has a count of zero, then you cannot select that alarm state.

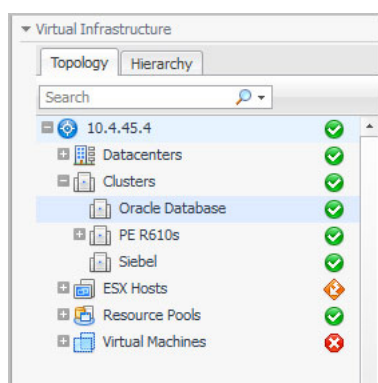
# Virtual Infrastructure view

The VMware Explorer dashboard provides a Virtual Infrastructure view. The Virtual Infrastructure view is located in the navigational panel at the left of the Foglight for Hyper-V browser interface, under Dashboards. For more information about the VMware Explorer dashboard, see [Use the VMware Explorer](#).

## Purpose

The Virtual Infrastructure view provides an organized view of the various virtual infrastructure objects that are monitored by agents. It serves as a navigation tool, and it also presents pertinent alarm information.

**Figure 53. Virtual Infrastructure view**



When you select an object from the Virtual Infrastructure view, all of the views in the VMware Explorer dashboard are updated with information pertaining to that object.

## Content and embedded views

The Virtual Infrastructure view contains two tabs views: the Topology tab and the Hierarchy tab.

Within the Topology view, all of the virtual infrastructure objects are organized into a tree using object type (or topology type) containers for branches. The top-level objects in the Topology view are always the VirtualCenters or vCenter@.

Within the Hierarchy view, each VirtualCenter object is organized into a tree that has the same hierarchical structure as the VirtualCenter and displays the objects (datacenters, clusters, resource pools, virtual machines, folders, etc.) within the VirtualCenter as branches.

## Description of embedded views

The Virtual Infrastructure view is made up of the following embedded views:

- [Topology tab](#)
- [Hierarchy tab](#)
- [Mouse-over status popups](#)

## Topology tab








The Topology view is organized into a tree using object type (or topology type) containers for branches.

The top-level objects in the Topology view are always the VirtualCenters.

Each VirtualCenter in the Topology view contains several object type containers, and each object type container contains every object of that particular type that is managed by the parent VirtualCenter.

Each object type container, as well as each object, has a representative icon that is displayed to the left, as shown in the following table.

Table 1. Virtual Infrastructure View Object Icons

Icon	Object	Object Name
	VirtualCenter	VMWVirtualCenter
	Datacenter	VMWDatacenter
	Cluster	VMWCluster
	ESX Server	VMWESXServer
	Resource Pool	VMWResourcePool
	Virtual Machine	VMWVirtualMachine
	Datastore	VMWDatastore

At the right, the Topology view displays status indicators. For an individual object, the status indicator represents the alarm of highest severity that is outstanding for that object. For an object type container, the status indicator represents the alarm of highest severity that is outstanding for all of the objects of that type.

**i** **NOTE:** A single virtual machine running at a high CPU utilization does not trigger an alarm for its parent ESX® Server. An alarm is only triggered for the parent ESX Server if the server itself is running at a high CPU utilization.

## Hierarchy tab

The Hierarchy view represents the logical layout of VirtualCenter management servers, so it is not organized into groups of common objects.

In the Hierarchy view, each VirtualCenter object is organized into a tree that has the same hierarchical structure as the corresponding VirtualCenter, displaying the objects (for example, datacenters, clusters, resource pools, virtual machines, and folders) within the VirtualCenter as branches.

Each object in the Hierarchy view has a representative icon that is displayed at the left of the object's name. These icons are shown in the table in [Topology tab](#) on page 79.

At the right, the Hierarchy view displays status indicators. Each status indicator represents the alarm of highest severity that is outstanding for the corresponding object.

## Mouse-over status popups

When you hover the cursor over an object in the Virtual Infrastructure view, you see a popup that provides a summary of the present state of that object.

The following image shows the popup you see when you hover the cursor over a VirtualCenter object in the Virtual Infrastructure view.



Figure 54. Status popup example

<b>Datacenters</b>	4				
		0	0	1	3
<b>Clusters</b>	5				
		0	0	0	5
<b>ESX Hosts</b>	5				
		1	0	0	4
<b>Resource Pools</b>	22				
		0	0	2	20
<b>Datastores</b>	21				
		0	0	1	20
<b>Virtual Machines</b>	148				
		3	21	45	90

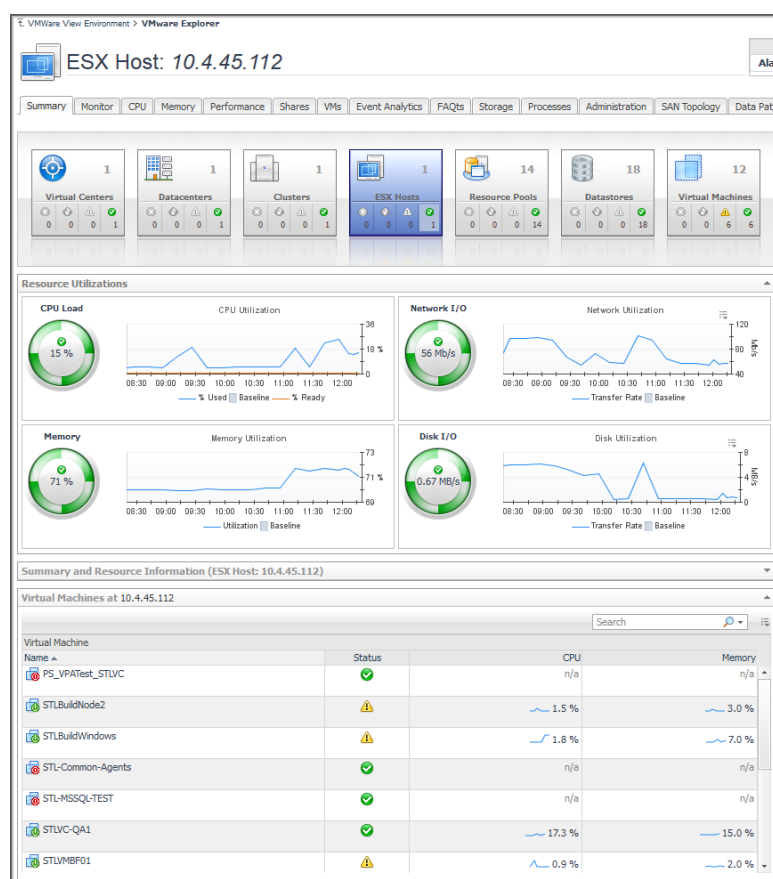
## VMware Explorer Primary view

The VMware Explorer dashboard has a Primary view that takes up the entire display panel of the browser interface. For more information about the VMware Explorer dashboard, see [Use the VMware Explorer](#).

### Purpose

The VMware Explorer Primary view is the most content-intensive view in Foglight for VMware Horizon View. It provides access to summary (of alarm, resource, and other) information for the object being viewed in the VMware Explorer dashboard, as well as detailed information on performance with respect to the four core ESX® infrastructure resources: CPU, memory, disk, and network usage. This view provides a great deal of value to administrators who leverage to monitor their virtual infrastructure.

**Figure 55. VMware Explorer Primary view**



It provides navigation tabs that can be used to view a variety of valuable information pertaining to the object being viewed.

## Content and embedded views

The metrics and the amount of detail displayed in the Primary view vary depending on the type of object you select.

The Primary view changes in appearance and content, depending on which navigation tab and embedded view you have selected.

The VMware Explorer Primary view heading, located at the top of the VMware Explorer Primary view, consists of three main components:

- an icon and text that specify the type of selected object or object container (from this point on, these two are referred to simply as object, unless otherwise specified).
- an alarm summary for the selected object.
- navigation tabs.

The alarm summary at the right of the Primary view heading shows you the number of alarms at each severity level that are outstanding for the selected object. When you click an alarm count, you get a popup that lists the active alarms for the object.

The navigation tabs are located immediately below the selected object's name. These navigation tabs vary from object to object, but generally contain a tab to an object summary (typically the default view), a tab to an object performance overview, and one or more tabs to other relevant information.

The Primary view changes in appearance and content, depending on which navigation tab and embedded view you have selected. For example, typically if you select an object type container from the Topology view, the Summary tab in the Primary view displays a consumption graph and a table that are representative of the group of

objects within that container. However, if you select a Resource Pools container from the Topology view, the Summary tab in the Primary view displays a Resource Pools Relationship Tree that contains every resource pool that belongs to the clusters within the associated VirtualCenter.

If you select an individual resource pool from the Virtual Infrastructure view, the Summary tab in the Primary view displays summary and utilization information for that resource pool. This is typically the type of information you see for the Summary tab when you select any individual object from the Virtual Infrastructure view.

The metrics and the amount of detail displayed in the Primary view vary depending on the type of object you select.

The VMware Explorer Primary view is a combination of a number of different embedded views. For more information, see the following topics:

- [Administration tab](#)
- [Cost tab](#)
- [CPU tab](#)
- [Event Analytics tab](#)
- [FAQs view](#)
- [Memory tab](#)
- [Monitor tab](#)
- [Performance tab](#)
- [Processes tab](#)
- [Related Objects views](#)
- [Resource Pools Relationship Tree view](#)
- [Shares tab](#)
- [Storage tab](#)
- [Summary tab](#)
- [Utilizations views](#)

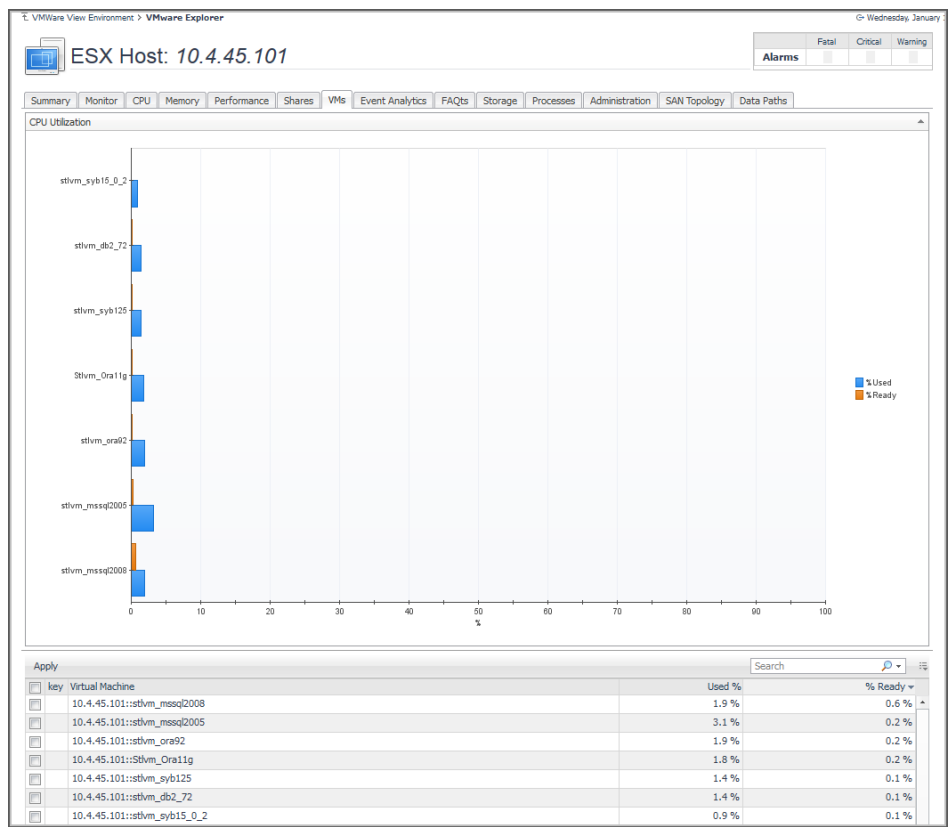
## VMs tab

This tab is available in the VMware Explorer. To find it, open the VMware Explorer and on the [Virtual Infrastructure view](#), that appears on the navigation panel, select any node, except the individual virtual machine nodes. In the VMware Explorer, open the **VMs** tab.

### Purpose and content

The VMware Explorer's **VMs** tab displays the combined CPU utilization for all virtual machines associated with the selected component. This includes the percentages of CPU processing power allocated to the virtual machines that is used and ready for use.

Figure 56. VMs tab



## Description of embedded views

This view is made up of the following embedded views:

- [CPU Utilization](#)
- [Virtual Machines](#)

## CPU Utilization

This view shows the percentages of CPU processing power that is used and ready for use, for each virtual machine that is associated with the selected component during the selected time period.

## Virtual Machines

This view shows a list of all virtual machines that are associated with the selected component. It displays the names and percentages of CPU processing power that is used and ready for use, for each virtual machine.

## We are more than just a name

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

## Our brand, our vision. Together.

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

## Contacting Quest

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

## Technical support resources

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

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

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