Quest

Quest® Change Auditor for VMware ® 7.0

User Guide

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. All other trademarks and registered trademarks are property of their respective owners.

Legend

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

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

Change Auditor for VMWare User Guide
Updated - August 2019
Software Version - 7.0

Contents

1

Change Auditor for VMWare Overview

- Introduction
- Features and benefits
- Deployment requirements

Introduction

Proper auditing and log management for your VMware vCenter Server infrastructure components are critical for security and compliance, but they can prove nearly impossible in practice using native auditing tools.

Because vCenter was designed as a management application, not a security application, it lacks the granularity in policy enforcement required for secure deployments. And because there is no central console, you have got to repeat each process for each server, and you end up with a huge volume of data and a myriad of reports. That means proving compliance or reacting quickly to events is a constant challenge.

Your data security is also at risk because native event details are sparse and difficult to interpret. As a result, you may not find out about problems until it is too late. Moreover, because native trails can be deleted or overwritten, the integrity of the log data can be compromised — defeating the purpose of auditing in the first place. As a result, even the most skilled and diligent vCenter-based organizations are often left exposed to the security risks associated with inadequate auditing and log management.

VMware auditing helps you ensure the security, compliance and control of event activity and the security of VMware vCenter. It manages, audits, reports and alerts on vital changes to VMware's infrastructure, including data centers, hosts, virtual machines and other resources associated with vCenter or ESX hosts.

NOTE: Throughout the product and documentation, references to 'ESX' means all supported versions of ESX and ESXi.

This guide has been prepared to assist you in becoming familiar with Change Auditor for VMware. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

- For information on the core functionality available in Change Auditor regardless of the product license that has been applied, see the Change Auditor User Guide and the Change Auditor Installation Guide.
- For event details, see the Change Auditor for VMware Event Reference Guide.

Features and benefits

- Audit all critical changes

  Extensive, customizable auditing and reporting for all critical changes to vCenter configuration settings, ESX hosts, folders, clusters, resource pools, virtual machines and users. You will get complete visibility into all changes over the course of time and in chronological order with in-depth forensics on who, what, when, where, and why including before and after values. With real-time alerts to any device, you will maintain constant awareness and the ability to respond to vital changes as they occur.

- Track user activity

  Tightens enterprise-wide auditing and compliance policies by tracking user and administrator activity such as additions, deletions, or changes to resources. With in-depth analysis and reporting capabilities, your vCenter infrastructure is protected from exposure to suspicious behavior or unauthorized access, and is always in compliance with corporate and government standards.

- Turn irrelevant data into meaningful information to drive security and compliance

  Eliminates guesswork-analysis reporting by translating isolated cryptic data into a series of meaningful events. You instantly get all information on the change you are viewing and all related events such as what other changes came from specific users. You also gain a better understanding of event trends with the ability to view, highlight and filter related events over the course of days, months and even years.

- Automate reporting for corporate and government regulations

  Utilizing Microsoft's SQL Reporting Services (SRS), Change Auditor for VMware vCenter provides clean, meaningful security and compliance reports on the fly. With a built-in compliance library and you can easily build your own custom reports, proving compliance for standards such as Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA) and Statement on Auditing Standards No. 70 (SAS 70).

Deployment requirements

For a successful deployment, ensure that your environment meets the minimum system requirements. For information on Change Auditor system requirements, see the Change Auditor Release Notes. For details on installing Change Auditor, see the Change Auditor Installation Guide.

2

Getting Started

Introduction

Change Auditor for VMWare provides you with the ability to search, report and alert on changes to VMware's infrastructure, including data centers, hosts, virtual machines and other resources associated with vCenter or ESX hosts.

This section provides a high-level view of the tasks to get you started using Change Auditor for VMware. To capture VMware events in Change Auditor, you must:

- Create VMware Auditing templates to define which VMware hosts to audit, which operations to capture, and the agent to use to audit these hosts.
- Enable the required VMware events.

Create a VMware template

To create a VMware auditing template:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **VMware** (under the Applications heading in the Auditing task list) to open the VMware Auditing page.
4. Click **Add** to open the VMware Auditing wizard which steps you through the process of creating a VMware Auditing template.
5. On the first page of the wizard, enter the following information:
    - **Template Name** — Enter a name for the template.

- **VMware Host** — Enter the IP address or name (the name must be resolvable) of the vCenter Server or of an individual host computer to audit. Click **Add** to add it to the VMware Host list.

  NOTE: To audit one or more hosts on a specific vCenter Server, use the **Find ESX Hosts** button to search for and select the ESX hosts to be audited. Clicking this button displays the Find ESX Hosts dialog, where you enter the information/credentials for the vCenter Server for which you want to view ESX hosts. After entering the vCenter Server information/credentials, click **Search** to retrieve a list of hosts. Select one or more hosts from the list and click **OK** to save your selection and close the dialog. The selected hosts will now be display in the VMware Host list in the auditing wizard.

Repeat this step to add additional VMware hosts to the list.

6 Click **Next** to select the agent to use for VMware auditing.

7 On the second page of the wizard, click **Browse**.

On the Eligible Change Auditor for VMWare Agents dialog, select the agent to use to monitor the selected VMware hosts.

NOTE: The agent must have access to the vCenter Server or VMware hosts selected on the first page of the wizard.

Once you have selected an agent, click **OK** to save your selection and close this dialog. Back on the wizard page, the agent information (Agent, Domain and Agent FQDN) is displayed for the selected Change Auditor for VMWare agent.

8 Click **Set Credentials** and enter the credentials to access the selected vCenter Server or VMware hosts. After entering the credentials, click **OK** to close the credentials dialog.

IMPORTANT: You can select an account with 'Read-Only' access or role (for restrictions) to properly audit VMware events. The credentials entered may be Active Directory or Linux credentials depending on the computer (vCenter Server vs. individual host computer) selected for auditing.

If you specified multiple machines (for example, vCenter Servers and/or ESX hosts) in the auditing template, all of these machines must use the same credentials.

A desktop notification indicates whether access is granted or denied to the specified vCenter Server or VMware host based on the credentials entered.

9 When valid credentials are entered, a Certificate Notice is displayed for each computer selected for auditing. Click **OK** to accept the certificates. Once valid credentials are supplied and the certificates have been accepted, click **Finish** to create the template.

10 On the Administration Tasks tab, click **Configuration**. Select **Agent** in the Configuration task list to open the Agent Configuration page.

11 Select the agent assigned to the VMware Auditing template (**Auditing** appears in the **VMware** column) and click **Refresh Configuration** to ensure the agent is using the latest configuration.

Enable and disable VMware events as required

Change Auditor for VMWare allows you to enable or disable events to best suit your organization. To view or modify the current event auditing settings, use the Audit Events page, which is accessible through the Administration Tasks tab.

To disable/enable individual events:

1 Open the Administration Tasks tab.

2 Click **Auditing**.

3 Select **Audit Events** (under the Configuration heading in the Auditing task list) to display the Audit Events page.

4 To disable an event, use one of the following methods:

- Select one or more enabled events and click **Disable**. (Use the **Shift** or **Ctrl** keys to select multiple events.)
- Select an enabled event, place your cursor in the corresponding **Status** cell, click the arrow control and select **Disabled** from the drop-down menu.
- Right-click an enabled event and select **Disable**.

5 To enable an event, use one of the following methods:

- Select one or more disabled events and click **Enable**. (Use the **Shift** or **Ctrl** keys to select multiple events.)
- Select a disabled event, place your cursor in the corresponding **Status** cell, click the arrow control and select **Enabled** from the drop-down menu.
- Right-click a disabled event and select **Enable**.

NOTE: You can also disable or enable an event using the **Disable/Enable** tool bar button at the top of the Event Details pane on a Search Results page.

Make changes and run a report

1 To test VMware auditing, make some changes to the host being monitored.

For example:

- start and stop a virtual computer
- create a new virtual computer

2 Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client** to review the events generated.

3 Open the **Searches** tab.

4 Expand the **Shared | Built-in | VMware** folder in the left pane.

5 Locate and double-click **All VMware Events in the last 7 days.**

A new Search Results tab is added to the client displaying the events that were captured.

6 Double-click an event from the Search Results grid to display the event details for the selected event.

Troubleshooting

If the VMware events do not appear as expected, check the following:

- Verify that the auditing template is applied. To ensure events are being captured, check to see if the Change Auditor agent assigned to the VMware Auditing template is using the latest agent configuration.

  NOTE:

  To verify that latest agent configuration is being used:

  1. Click **Start | All Programs | Quest | Change Auditor | Change Auditor Client**.
  2. Open the Administration Tasks tab (**View | Administration** menu command).
  3. If not already selected, click **Configuration**.
  4. Select **Agent** in the Configuration task list to open the Agent Configuration page.
  5. Select the agent assigned to the VMware Auditing template (**Auditing** appears in the **VMware** column) and click **Refresh Configuration**.

- Restart the agent.
- Ensure that if you add multiple computers (such as vCenter Servers and/or ESX hosts) to a single auditing template, all of these machines are using the same credentials. (To audit computers that use different credentials, you must create a VMware Auditing template for each.)

3

VMware Auditing

Introduction

The VMware Auditing page on the Administration Tasks tab displays details about each auditing template created and allows you to add new auditing templates.

This chapter provides a description of the Auditing page and Auditing wizard. For a description of the dialogs mentioned, see the online help. For more information about agent configurations, see the Change Auditor User Guide.

VMware Auditing page

The VMware Auditing page is displayed when **VMware** is selected from the Auditing task list in the navigation pane of the Administration Tasks page. From this page you can launch the VMware Auditing wizard to define templates specifying the VMware hosts to be audited. You can also edit existing templates, disable/enable templates and delete templates that are no longer being used.

The VMware Auditing page contains an expandable view of all the VMware Auditing templates that have been previously defined. To add a new template to this list, use the **Add** tool bar button. Once added, the following information is displayed for the template:

Template

Displays the name assigned to the template when it was created.

Status

Indicates whether the template is enabled or disabled. To enable/disable the template, place your cursor in this **Status** cell, click the arrow control and select the appropriate option from the drop-down menu.

Agent

Displays the name of the agent assigned to audit the selected VMware hosts.

User

Displays the name of the user being used to access the VMware hosts that are being audited.

VMware Hosts

This field is used for filtering data. Click the expansion box to the left of the Template name to expand this view and display additional details about an auditing template.

VMware Host

Displays the name or IP address of the vCenter Server™ or VMware host being audited, as entered on the first page of the wizard.

Status

Indicates whether auditing of the selected host is enabled or disabled.

Port

Displays the port number being used to access the selected vCenter Server or VMware host.

NOTE: The cells directly under the main heading rows are used for filtering data. That is, as you enter characters into these cells, the client will redisplay the templates that meet the search criteria (For example, comparison operator and characters entered). For more details about using the data filtering function provided throughout Change Auditor, see the Change Auditor User Guide.

VMware Auditing templates

To enable VMware auditing, first create a VMware Auditing template which specifies the VMware hosts to audit and the agent used to monitor the selected VMware hosts.

NOTE: If you add multiple machines (such as vCenter Servers and/or ESX hosts) to a single auditing template, all of these machines must use the same credentials. If you want to audit machines that use different credentials, you must create a different VMware Auditing template for each of these machines.

To create a VMware auditing template:

1. Open the Administration Tasks tab.
2. Click **Auditing**.
3. Select **VMware** (under the Applications heading in the Auditing task list) to open the VMware Auditing page.
4. Click **Add** to open the VMware Auditing wizard which will step you through the process of creating a VMware Auditing template.
5. On the first page of the wizard, enter the following information:
   - **Template Name** - Enter a name for the template.
   - **VMware Host** - Enter the IP address or name (the name entered must be resolvable) of the vCenter Server or of an individual host computer to be audited and click **Add** to add it to the VMware Host list.

     NOTE: To audit one or more hosts on a specific vCenter Server, use the **Find ESX Hosts** button to search for and select the ESX hosts to be audited. Clicking this button displays the Find ESX Hosts dialog, where you will be asked to enter the information/credentials for the vCenter Server for which you want to view ESX hosts. After entering the vCenter Server information/credentials, click **Search** to retrieve a list of hosts. Select one or more hosts from the list and click **OK** to save your selection and close the dialog. The selected hosts will now be displayed in the VMware Host list in the auditing wizard.

   Repeat this step to add additional VMware hosts to the list.
6. Click **Next** to select the agent to be used for VMware auditing.

7 On the second page of the wizard, click **Browse**.

On the Eligible Change Auditor for VMWare Agents dialog, select the Change Auditor for VMWare agent to be used to monitor the selected VMware hosts.

> **NOTE:** The Change Auditor for VMWare agent must have access to the vCenter Server or VMware hosts selected on the first page of the wizard.

Once you have selected an agent, click **OK** to save your selection and close this dialog. Back on the wizard page, the agent information (Agent, Domain and Agent FQDN) is displayed for the selected Change Auditor for VMWare agent.

8 Click **Set Credentials** and enter the credentials to be used to access the selected vCenter Server or VMware hosts. After entering the credentials, click **OK** to close the credentials dialog.

> **IMPORTANT:** You can select an account with 'Read-Only' access or role (for restrictions) to properly audit VMware events. The credentials entered may be Active Directory or Linux credentials depending on the computer (vCenter Server vs. individual host computer) selected for auditing.
>
> If you specified multiple machines (for example, vCenter Servers and/or ESX hosts) in the auditing template, all of these machines must use the same credentials.

A desktop notification indicates whether access is granted or denied to the specified vCenter Server or VMware host based on the credentials entered.

9 When valid credentials are entered, a Certificate Notice is displayed for each computer selected for auditing. Click **OK** to accept the certificates. Once valid credentials are supplied and the certificates have been accepted, click **Finish** to close the wizard and create the template.

10 On the Administration Tasks tab, click **Configuration**. Select **Agent** in the Configuration task list to open the Agent Configuration page.

11 Select the agent assigned to the VMware Auditing template (**Auditing** appears in the **VMware** column) and click **Refresh Configuration** to ensure the agent is using the latest configuration.

> **NOTE:** If you do not refresh the agent's configuration, the agent will automatically check for a new agent configuration based on the polling interval setting (located on the System Settings tab of the Configuration Setup dialog). The default is every 15 minutes.

To disable a VMware Auditing template:

1 On the Auditing page, use one of the following methods to disable an auditing template:

- Place your cursor in the **Status** cell for the template to be disabled, click the arrow control and select **Disabled**.
- Right-click the template to be disabled and select **Disable**.

The entry in the **Status** column for the template will change to 'Disabled'.

2 To re-enable the auditing template, use the **Enable** option in either the **Status** cell or right-click menu.

To disable auditing for an individual VMware host:

1 On the VMware Auditing page, use one of the following methods to disable the auditing of a VMware host:

- Place your cursor in the **Status** cell for the host to be disabled, click the arrow control and select **Disabled**
- Right-click the host to be disabled and select **Disable**

The entry in the **Status** column for the host will change to 'Disabled'.

2 To re-enable the auditing of a host, use the **Enable** option in either the **Status** cell or right-click menu.

To delete a VMware Auditing template:

1 On the Auditing page, select the template to be deleted and click **Delete | Delete Template**.

2 A dialog will be displayed confirming that you want to delete the selected template. Click **Yes**.

VMware Auditing wizard

The VMware Auditing wizard is displayed when you click **Add** or **Edit** on the VMware Auditing page. From this wizard, specify the VMware hosts to be audited and the Change Auditor for VMWare agent to be used to monitor the selected VMware hosts.

The following table provides a description of the fields and controls in the VMware Auditing wizard.

NOTE: A red flashing icon indicates that you have not yet entered the required information. Hovering your cursor over this icon displays a tool tip explaining what needs to be entered.

Table 1. VMware Auditing wizard

Create or modify a VMware Auditing Template page Use the first page of the wizard to enter a name for the template and select the VMware hosts to be audited.	
Template Name	Enter a descriptive name for the VMware auditing template.
VMware Host	Enter the IP address or name (must be resolvable) of the vCenter Server or of a VMware host that is to be audited.
Add	After entering the IP address or name of a host in the VMware Host text box, click e **Add** to add the host to the VMware Host selection list.
Find ESX Hosts	Clicking this button displays the Find ESX Hosts dialog allowing you to search a vCenter Server to select the ESX hosts that are to be audited. On this dialog, enter the IP address or name (and port) of the vCenter Server for which you want to view ESX hosts. Click **Search** to retrieve a list of hosts on the selected vCenter Server. Select one or more hosts from the list and click **OK** to save your selection and close the dialog.
Remove	To remove a host from auditing, select it in the VMware Host selection list and click **Remove** to the right of the list box.
VMware Host selection list	This list box displays the following information about the VMware hosts selected for auditing. • **VMware Host** - Displays the IP address or name of the host selected for auditing. • **Port** - Displays the port to be used for communication. This will display the default SSL port (443). If this is not the correct port number for a host, use the arrow controls to change it.
Select Change Auditor for VMWare Agents page Use the second page of the wizard to select the agent to be used to monitor the selected VMware hosts and to enter the credentials to be used to access the VMware hosts. **NOTE:** If you select multiple hosts in an auditing template, all of the hosts selected must use common credentials.	

Table 1. VMware Auditing wizard

Browse	Displays the Eligible Change Auditor Agents dialog allowing you to select an agent from the list of deployed agents. **NOTE:** The Eligible Change Auditor for VMWare Agents dialog only lists eligible servers running .NET 4.5.2 Framework, which is a requirement for the agent selected to audit VMware. Once an agent is selected the following details are displayed: • Agent • Domain • Agent FQDN • User (after valid credentials have been entered using the **Set Credentials** button)
Set Credentials	Displays the VMware Host Credentials dialog allowing you to enter the credentials to be used to access the computers (vCenter Servers and/or hosts) selected on the first page of the wizard. **NOTE:** If you specified multiple machines (for example, vCenter Servers and/or ESX hosts) in the auditing template, all of these computers must use the same credentials. **NOTE:** Valid credentials must be entered in order to proceed.
Clear Credentials	Allows you to clear previously entered credentials.
Change Auditor for VMWare Agent	Once a Change Auditor for VMWare agent has been selected, the following information is displayed: • Agent • Domain • Agent FQDN • User

VMware events polling interval

From the Agent Configuration page on the Administration Tasks tab you can view and/or modify the VMware polling interval.

Use the VMware tab at the top of the Configuration Setup dialog to define the polling interval to be used to retrieve VMware events.

Polling Interval

This setting determines how often the agent will poll the VMware hosts for new VMware events. The default is every 60 seconds. Use the arrow controls to increase or decrease this value.

Valid range: 60 - 9999 seconds.

4

VMware Searches/Reports

Introduction

Change Auditor provides built-in searches that can be run to retrieve VMware activity captured by deployed agents enabling you to retrieve valuable information from a variety of perspectives.

NOTE: The terms ‘searches’ and ‘reports’ are used in conjunction to acquire the desired output. You run a ‘search’ and the results returned are referred to as a ‘report’.

You can also create custom search definitions to search for the configuration changes that need to be tracked in your environment. You will use the search properties tabs across the bottom of the Searches page to define new custom searches.

For a description of the dialogs mentioned in this chapter, please refer to the online help. For a description of the Search Properties tabs and how to use these tabs to customize your searches, see the Change Auditor User Guide.

VMware built-in searches

This section provides procedures for running built-in searches and provides a description of the details displayed on the Search Results page for VMware events.

NOTE: By default, the VMware reports include the following information on the Search Results page: VMware Audited Host, VMware Host, VMware Datacenter, and VMware Virtual Machine. These additional columns are defined using the Layout tab.

To see a complete list of built-in reports, see the Change Auditor Built-in Reports Reference Guide.

To run a built-in search:

1. Click the **Searches** tab or select **View | Searches**.
2. Expand and select the appropriate folder in the explorer view (left pane) to display the list of search definitions stored in the selected folder. For example, selecting the **Shared | Built-in | Cloud Storage Activity** will display all the built-in searches available for Cloud Storage.
3. In the right-hand pane, locate the search to be run and use one of the following methods to run the selected search:
   - Double-click a search definition
   - Right-click a search definition and select **Run**
   - Select the search definition and click **Run**

4 A new Search Results Page will be displayed populated with the audited events that met the search criteria defined in the selected search definition.

NOTE: To modify a built-in search, see the Change Auditor User Guide.

Create custom searches

The following scenarios explain how to use the What tab to create custom VMware searches.

NOTE: If you wanted to, you can use the other search properties tabs to define additional criteria:

- Who - allows you to search for events generated by a specific user, computer or group
- Where - allows you to search for events captured by a specific agent or within a specific domain or site
- When - allows you to search for events that occurred within a specific date/time range
- Origin - allows you to search for events that originated from a specific workstation or server

NOTE: Selecting the **Private** folder will create a search that only you can run and view, whereas selecting the **Shared** folder will create a search which can be run and viewed by all Change Auditor users.

To search for all events:

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

3 Click **New** to activate the Search Properties tabs across the bottom of the Searches page.

4 On the Info tab, enter a name and description for the search.

5 Open the What tab, expand **Add** and select **Subsystem | VMware**.

6 On the **Add VMware Host** dialog, select the **All VMware Hosts** option.

7 Review the Actions section and select those that are to be included in the search.

By default, **All Actions** is selected meaning that all of the actions associated with the VMware host will be included in the search.

8 Click **OK** to save your selection and close the dialog.

9 Once you have defined your search criteria, click **Run** to save and run the search.

10 When this search is run, Change Auditor will search for all VMware events and display the results in a new search results page.

To search for events performed against a specific VMware host:

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

3 Click **New** to activate the Search Properties tabs across the bottom of the Searches page.

4 On the Info tab, enter a name and description for the search.

5 Open the What tab, expand **Add** and select **Subsystem | VMware**.

6 On the Add File System Path dialog, select one of the following scope options:

- **This Object** - select to search only the selected object.

7 In the **Host Name** field, enter or use the filters to select the host to be searched.

8 In the **VM Name** field, enter or use the filters to select the VM to be searched.

9 Review the Actions section and select those that are to be included in the search.

By default, **All Actions** is selected meaning that all of the actions associated with the path will be included in the search.

10 Click **OK** to save your selection and close the dialog.

11 Click **Run** to save and run the search. Click **Save** to save the search definition without running it.

12 When this search is run, Change Auditor will search for VMware events in the host and VM.

To search for a specific event class:

1 Open the Searches page.

2 In the explorer view (left pane), expand and select the folder where you want to save your search.

3 Click **New** to activate the Search Properties tabs across the bottom of the Searches page.

4 On the Info tab, enter a name and description for the search.

5 Open the What tab, click **Add** (or expand **Add** and select **Event Class**).

6 On the Add Facilities or Event Classes dialog, enter **VMware** in the data filter field under the Facility heading to display all of the VMware events.

7 From this list, select one or more events and use the **Add | Add This Event** option to add the selected events to the list box at the bottom of the dialog. Click **OK** to save your selection and close the dialog.

8 Click **Run** to save and run the search. Click **Save** to save the search definition without running it.

9 When this search is run, Change Auditor will search for the VMware events based on the search criteria specified on the What tab and display the results in a new search results page.

Search results

The VMware event information (including key information like who, what, when, where, why, the event origin, and the file and cloud storage information) can be viewed on the Event Details pane.

Table 2. Event Details pane: VMware events

ChangeAuditor	Description
Severity	Displays “Low”, “Medium”, or “High” depending on the event.
Who	Specifies the name of the user who initiated the change.
When	Specifies the date and time when the change occurred.
Where	Displays the name of the workstation where the change occurred.
Source	Displays ‘Change Auditor’ which is the application from which the event was retrieved.
Origin	Displays the NetBIOS name and IP address of the workstation from which the event was generated.
What	Displays a description of the activity that occurred. **NOTE:** For lengthy descriptions, hover your cursor over the description field to view the entire event description.
Facility	Displays that it is VMware session activity.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

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 www.quest.com/contact.

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.