Quest

Quest® InTrust 11.4.2

Preparing for Auditing VMware vCenter and ESX or ESXi

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 Web site (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**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

InTrust Preparing for Auditing VMware vCenter and ESX or ESXi
Updated - September 2020
Version - 11.4.2

Contents

VMware Auditing Overview

The VMware Knowledge Pack expands the auditing and reporting capabilities of InTrust to VMware vCenter, ESX and ESXi.

You can audit the following in your virtual environments:

- Allocation of resources
- Management of security settings
- Status indicator changes

These capabilities help ensure that you can easily avoid denial-of-service situations in production-critical virtual environments.

Setup

Requirements

For details about the versions of VMware environments that InTrust can audit, see the following topics:

- VMware ESX and ESXi Events
- VMware vCenter Events

Components

Auditing of VMware virtual environments is achieved by installing the VMware vCenter and ESX/ESXi Knowledge Pack. The Knowledge Pack contains the following InTrust objects:

- Data sources:
  - VMware vCenter events
  - VMware ESX and ESXi events
- Sites:
  - Microsoft Windows Network\VMware vCenter Servers
  - Unix Network\VMware ESX and ESXi Servers
- Gathering policies:
  - Microsoft Windows Network\VMware vCenter
  - Unix Network\VMware ESX and ESXi
- Import policies:
  - Windows Network\VMware vCenter
  - Unix Network\VMware ESX and ESXi
- Tasks:
  - VMware vCenter weekly event collection
  - VMware ESX and ESXi weekly event collection

The Knowledge Pack also includes reports:

- Virtual machine startups and shutdowns
- Virtual machine reconfigurations
- Virtual machine snapshot activity

- Virtual machine creations and deletions
- VMware All Events
- VMware ESX Configuration Changes
- VMware Permission Changes
- VMware User Logon and Logoff

Installation

The VMware vCenter and ESX/ESXi Knowledge Pack must be installed on top of an existing InTrust installation.

Specifying What Computers to Use for Event Processing

The choice of event-processing computers depends on whether you expect the InTrust server to have any trouble allocating enough system resources to process events from VMware systems. The workload of processing the other platforms may be such that you may want to consider a dedicated InTrust server for VMware environment auditing.

You have only a few virtualization servers

In this case, all of the event processing can be done by the InTrust server that also performs auditing activity for other platforms. This means that you will later need to specify this server as the hosting server for your gathering jobs.

You have a lot of virtualization servers

In this case, consider setting up an additional InTrust server, as described in the InTrust Deployment Guide, in Installing Servers into Existing InTrust Organization. Later, you will specify this server as the hosting server for your gathering jobs.

Specifying Where to Look

This topic describes how to specify the vCenter and ESX (ESXi) servers for auditing. This step involves using InTrust Manager to include the servers you want to audit in InTrust sites. Note the following specifics:

- vCenter servers must be members of sites in the Configuration | Sites | Microsoft Windows Network container.
- ESX and ESXi servers must be members of sites in the Configuration | Sites | Unix Network container.

This topic describes the following configuration options:

- For vCenter servers:
  - Single server
  - Multiple servers

- For ESX and ESXi servers:
    - Single server
    - Multiple servers

See the option or options that fit your environment, and take the suggested steps.

Single vCenter Server

To audit a single vCenter server, take the following steps in InTrust Manager:

1. Include the server in the predefined "VMware vCenter Servers" site.
2. Make a copy of the predefined "VMware vCenter weekly event collection" task, and give it a suitable name.
3. Set and enable the schedule for the new task as necessary.
4. In the properties of the "VMware vCenter Servers" site, specify the credentials to use for connecting to the vCenter server in the **To access site objects, use** option group. Make sure that the account you use is a member of at least the **Read-only** role on the vCenter server.
5. Commit your changes.

NOTE: This procedure assumes that the InTrust objects related to vCenter auditing have default configurations. If the configuration of the "VMware vCenter events" data source has been edited, make sure that the **Use Integrated Windows Authentication** parameter of this data source is set to **1**. This setting is located in the data source properties, on the **Parameters** tab.

A value of **1** means that the data source will inherit access credentials from the site for which they are set (see step 4). Generally, credentials are passed on along the following path: **InTrust server | task | job | site | data source**, and can be overridden at the level of any of these objects if the object supports it.

If the **Use Integrated Windows Authentication** parameter is enabled while a gMSA is used as the InTrust server account, make sure the gMSA is not inherited as the access account for site objects. Instead, override the access credentials with an explicitly specified account. This can be done at site level (in the site properties) or at job level, and so on.

Multiple vCenter Servers

If access credentials are shared by all vCenter servers

To audit multiple vCenter servers that accept the same access credentials, take the following steps in InTrust Manager:

1. Include all the servers in the predefined "VMware vCenter Servers" site.
2. Make a copy of the predefined "VMware vCenter weekly event collection" task, and give it a suitable name.
3. Set and enable the schedule for the new task as necessary.
4. In the properties of the "VMware vCenter Servers" site, specify the credentials to use for connecting to the vCenter server in the To access site objects, use option group. Make sure that the account you use is

a member of at least the Read-only role on the vCenter server.

5. Commit your changes.

NOTE: This procedure assumes that the InTrust objects related to vCenter auditing have default configurations. If the configuration of the "VMware vCenter events" data source has been edited, make sure that the **Use Integrated Windows Authentication** parameter of this data source is set to **1**. This setting is located in the data source properties, on the **Parameters** tab.

A value of **1** means that the data source will inherit access credentials from the site for which they are set (see step 4). Generally, credentials are passed on along the following path: **InTrust server | task | job | site | data source**, and can be overridden at the level of any of these objects if the object supports it.

If the **Use Integrated Windows Authentication** parameter is enabled while a gMSA is used as the InTrust server account, make sure the gMSA is not inherited as the access account for site objects. Instead, override the access credentials with an explicitly specified account. This can be done at site level (in the site properties) or at job level, and so on.

If access credentials differ across the vCenter servers

To audit multiple vCenter servers for which access credentials differ, take the following steps in InTrust Manager:

1. Create copies of the predefined "VMware vCenter Servers" site so that there is one site for each vCenter server access account. Name the sites accordingly.
2. Populate the sites as necessary. Include multiple vCenter servers in a site only if these servers share the same access credentials.
3. Make a copy of the predefined "VMware vCenter weekly event collection" task, and give it a suitable name.
4. Set and enable the schedule for the new task as necessary.
5. Inside the task, create copies of the predefined gathering job so that there is one job for each vCenter server access account. Name the jobs accordingly.

Then, do the following for each of the jobs you have created:

1. In the job properties, on the **Gathering** tab, select the correct site to gather events from.
2. Make sure that the **Use agents to execute this job on target computers** option is turned off.
3. Open the properties of the site that the job uses, and in the **To access site objects, use** option group, supply the account to use for the vCenter connection.

After you have completed the configuration, commit your changes.

NOTE: This procedure assumes that the InTrust objects related to vCenter auditing have default configurations. If the configuration of the "VMware vCenter events" data source has been edited, make sure that the **Use Integrated Windows Authentication** parameter of this data source is set to **1**. This setting is located in the data source properties, on the **Parameters** tab.

A value of **1** means that the data source will inherit access credentials from the site for which they are set. Generally, credentials are passed on along the following path: **InTrust server | task | job | site | data source**, and can be overridden at the level of any of these objects if the object supports it.

Single ESX or ESXi Server

To audit a single ESX or ESXi server, take the following steps in InTrust Manager:

1. Include the server in the predefined "VMware ESX and ESXi Servers" site.
2. In the properties of the predefined "VMware ESX and ESXi events" data source, on the **Parameters** tab, use the **User Name** and **Password** parameters to specify the credentials for connecting to the virtualization server. Make sure that the account you use is a member of at least the **Read-only** role on the virtualization server.
3. Make a copy of the predefined "VMware ESX and ESXi weekly event collection" task, and give it a suitable name.
4. Set and enable the schedule for the new task as necessary.
5. Commit your changes.

Multiple ESX or ESXi Servers

If access credentials are shared by all ESX and ESXi servers

To audit multiple ESX or ESXi servers that accept the same access credentials, take the following steps in InTrust Manager:

1. Include all the servers in the predefined "VMware ESX and ESXi Servers" site.
2. In the properties of the predefined "VMware ESX and ESXi events" data source, on the **Parameters** tab, use the **User Name** and **Password** parameters to specify the shared credentials for connecting to the virtualization servers. Make sure that the account you use is a member of at least the **Read-only** role on the virtualization servers.
3. Make a copy of the predefined "VMware ESX and ESXi weekly event collection" task, and give it a suitable name.
4. Set and enable the schedule for the task as necessary.
5. Commit your changes.

If access credentials differ across the ESX and ESXi servers

To audit multiple ESX and ESXi servers for which access credentials differ, take the following steps in InTrust Manager:

1. Create copies of the predefined "VMware ESX and ESXi Servers" site so that there is one site for each server access account. Name the sites accordingly.
2. Create copies of the predefined "VMware ESX and ESXi events" data source so that there is one site for each virtualization server access account. Name the data sources accordingly.
3. Create copies of the predefined "VMware ESX and ESXi" gathering policy so that there is one policy for each virtualization server access account. Name the policies accordingly. Remove the predefined data source from the cloned policies.
4. Populate the sites as necessary. Include multiple ESX and ESXi servers in a site only if these servers share the same access credentials.

5. Make a copy of the predefined "VMware ESX and ESXi weekly event collection" task, and give it a suitable name.
6. Set and enable the schedule for the task as necessary.
7. Inside the task, create copies of the predefined gathering job so that there is one job for each server access account. Name the jobs accordingly.

Do the following for each of the data sources you have created:

1. In the data source properties, on the **Parameters** tab, use the **User Name** and **Password** parameters to specify the credentials for connecting to the virtualization server or servers. Make sure that the account you use is a member of at least the **Read-only** role on the virtualization server or servers.
2. Find the corresponding gathering policy that you have created, and add this data source to it.

Then, do the following for each of the jobs you have created:

1. In the job properties, on the **Gathering** tab, select the correct site to gather events from.
2. Select the correct gathering policy to use.
3. Make sure that the **Use agents to execute this job on target computers** option is turned off.

After you have completed the configuration, commit your changes.

Collecting Events and Reporting

By now, you have configured the connection between InTrust and the virtualization servers. To fine-tune the configuration of auditing and reporting, you can do the following:

What you want to do	What you should configure
Change the event gathering schedule	Edit the schedule in the properties of the task you are using.
Redirect events to different data stores	In the properties of the gathering job inside the task, change the audit database or repository.
Browse gathered events directly	Use InTrust Repository Viewer.
Make reports	In the task, add a final reporting job. Configure the properties of the job, such as the reports you want and report delivery settings.
View interactive reports	Use InTrust Knowledge Portal. To start working with Knowledge Portal, it is required to specify some of the security settings and data source properties. Before you can view reports, configure the data source to connect to the product database. Data sources are databases that store the information used in the reports. It is also required to configure access rights to provide the report users with access to reports they need. These rights are assigned through specifying appropriate SQL Reporting Services role to a user or group account. After Knowledge Portal is properly configured, open InTrust Manager and launch

What you want to do	What you should configure
	the task that includes a reporting job with the reports you need. Then in Knowledge Portal use the Reports tab. For detailed information, see the InTrust Deployment Guide.
Tweak the scope of events that are collected to filter out unnecessary data	Edit the repository of database filter in the properties of the data source or the policy that includes the data source. Policy filters are applied after data source filters.

Remember to commit the changes you make to InTrust configuration.

For details about the procedures suggested, see the InTrust Auditing Guide.

Use Scenarios

This topic describes typical situations in a production environment and how InTrust helps handle them. For more details, see the following:

- Tracking Pool Access Privileges
- Tracking Virtual Machine Removal

For information about specific procedures, such as creating tasks and jobs, see the InTrust Auditing Guide.

Tracking Pool Access Privileges

Suppose you have a single vCenter server, and your vCenter resources have been carefully rationed. The workload is currently approaching capacity. You need to make sure that only the current resource pool administrators make changes that affect vCenter performance, and these administrators make their changes responsibly.

For that purpose, prepare an auditing and reporting workflow that includes the following:

1. Daily gathering of events from the virtualization servers.
2. Reports on permission changes after each gathering session.

To set up event gathering

1. Make sure you have completed the steps outlined in the GettingStarted topic.
2. Change the schedule of the auditing task you have configured so that the task runs daily, preferably at a time when the load on the vCenter server is at its lowest. Rename the task accordingly.
3. Commit your changes.

To set up reporting

1. In the task, add a reporting job that is a successor of the gathering job.
2. While configuring the reporting job, select the "VMware Permission Changes" report, and specify your preferred delivery method.
3. Commit your changes.

For more details about reporting jobs, see the InTrust Auditing Guide.

Tracking Virtual Machine Removal

Removal of virtual machines is understandably a highly important action to watch out for. Such activity should be tracked very closely.

To set up event gathering

1. Make sure you have completed the steps outlined in the GettingStarted topic.
2. Change the schedule of the auditing task you have configured so that the task runs daily, preferably at a time when the load on the vCenter server is at its lowest. Rename the task accordingly.
3. Make sure that the gathering job inside the task gathers events to a repository.
4. Commit your changes.

To track virtual machine removal in Repository Viewer

1. Connect to the repository that contains events from the VMware environment.
2. Navigate to the events you need in the left-pane treeview.
3. In the column label row above the event list, click the leftmost icon to open the Field Chooser dialog box.
4. In the drop-down menu of the dialog box, select **Named Insertion Strings**.
5. In the list below, select **VM: EventType**. This insertion string contains textual information about the VMware-specific event type, so it is very useful for analyzing events from VMware systems.
6. Underneath the **VM: EventType** column name, change the operator to **Contains**, and type **removed** in the filter box.
7. View the filtered results and their details; sort and group them as necessary.

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

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