Quest

Quest® InTrust 11.5.1

Self-Auditing in InTrust

Contents

© 2024 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our 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 Self-Auditing in InTrust
Updated - February 2023
Version - 11.5.1

Self-Auditing in InTrust

InTrust provides self-auditing capabilities, which help you monitor the health of your InTrust deployment and meet regulations compliance requirements. Self-auditing is configured differently for InTrust servers and agents. For details, see the following topics:

- InTrust Server Self-Auditing
- InTrust Agent Self-Auditing
- Using Self-Audit Events

InTrust Server Self-Auditing

InTrust Server self-auditing covers requests for InTrust services by external client applications (such as InTrust Deployment Manager and Repository Viewer) and InTrust-specific inter-service communication that occurs locally on the InTrust server. For details about the events that are logged, see InTrust Self-Audit Events.

By default, self-auditing of InTrust servers is disabled. To turn it on and off or change the auditing level on a particular InTrust server, use the **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Aelita\ADC\RpcServer\RpcAuditLevel** registry value on that server. The following values are accepted:

- 0
  Self-audit disabled
- 1
  Remote Access: External calls to InTrust Server are audited; RPC calls from InTrust services on the same server are not audited
- 2
  Everything : All calls (both external and local) are audited

InTrust Agent Self-Auditing

Agent-related self-auditing provides information about how agents run real-time monitoring rules. This data gives you insights into the following types of activity, all of which are based on real-time rules:

- Real-time monitoring
- Real-time event collection
- Agent-side log backup

For details about the audited events, see InTrust Self-Audit Events.

To enable or disable agent self-auditing globally in your InTrust organization, set the **ITRT_SelfAuditLevel** organization parameter to **1** or **0**, respectively. For details about modifying InTrust organization parameters, see Organization Parameter Editor.

NOTE: You can override the enabled or disabled state of agent self-auditing on a per-server basis. However, this is not recommended, because there is no direct control over which agents respond to which InTrust server.

Using Self-Audit Events

InTrust lets you use its tools to collect and analyze its own self-audit events.

The following basic set of configuration objects is provided for this:

- "InTrust Self-Audit Log" data source
- "InTrust Self-Audit" search folder in Repository Viewer, containing the following searches:
    - Agent-side log backup configuration changes
    - All InTrust self-audit events
    - Connections to InTrust servers
    - Real-time collection configuration changes
    - Real-time monitoring configuration changes

Depending on which workflow you prefer, you can set up self-audit log management in InTrust Deployment Manager with collections or InTrust Manager with gathering jobs.

IMPORTANT: When you gather from InTrust servers, it is recommended that each InTrust server gather from itself. This helps avoid situations where two InTrust servers gather from one another, which causes errors due to internal limitations. For this reason, more configuration objects need to be created than would be necessary for auditing computers that are not InTrust servers.

Gathering with Collections

To set up InTrust self-audit log gathering in InTrust Deployment Manager, you need some collections that get the "InTrust Self-Audit Log" data source from your InTrust servers. For each of your InTrust servers, create a dedicated Windows collection and configure it as follows:

- Include the InTrust server that the collection is for. Specify the same server as the one that processes the collection, in the **Select InTrust Server** field.
- Select "InTrust Self-Audit" as the data source.
- Specify the repository you need as the data store. Use a single repository for all self-audit data.

For details about the particular procedures, see Managing Collections and, generally, Getting Started with InTrust.

Gathering with Jobs

To set up InTrust self-audit log gathering in InTrust Manager, configure the following set of objects:

- For each of your InTrust servers, create a dedicated site and include the server in it. Specify the same server as the one that processes the site, in the **InTrust Server** field. For details, see Creating Sites.
- Create a gathering policy and select "InTrust Self-Audit" as its only data source. For details, see Understanding Policies.
- Create a dedicated task for gathering self-audit events and provide a suitable schedule for it. For details, see Understanding Jobs and Tasks.
- Within this task, create one gathering job for each of your new sites (see Gathering Job for details) and configure it as follows:
    - Bind your new policy to the site that the job is for.
    - Specify the repository you need as the data store. Use a single repository for all self-audit data.
- Apply your changes by clicking the **Commit** button in the toolbar.

For general information about task-based gathering workflows, see the Auditing Guide.

Analyzing Self-Audit Data in Repository Viewer

To view self-audit events collected to a repository, open it in Repository Viewer and use the predefined searches in the "InTrust Self-Audit" search folder. For details, see Running Searches and, generally, Searching for Events in Repository Viewer.

About us

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