Quest® InTrust 11.6.1

Contingency Planning Guide

© 2024 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our 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

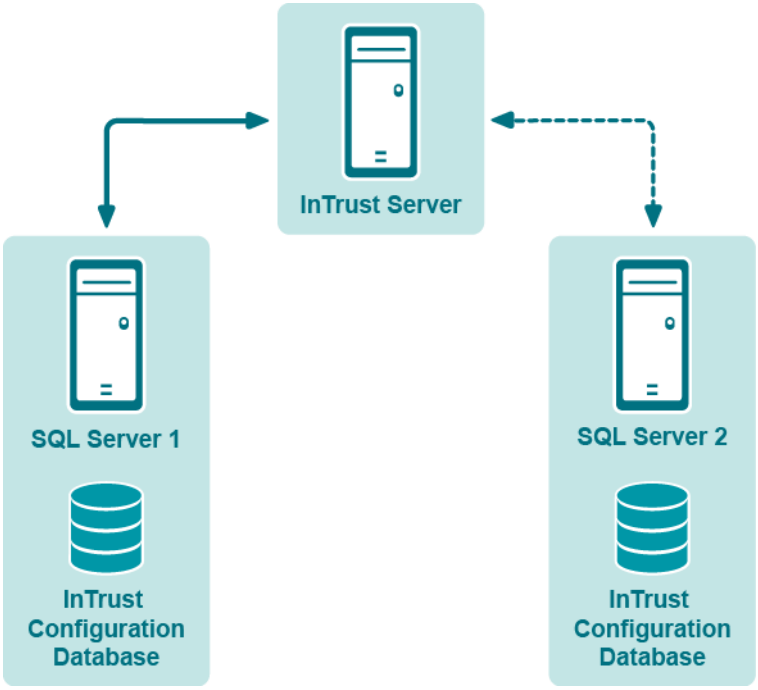
CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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

InTrust Contingency Planning Guide
Updated - September 2024
Version - 11.6.1

Contents

Contingency Planning Overview



Looking at any InTrust organization infrastructure, it is possible to determine the components which are the most critical for the InTrust operation. In case these components are damaged due to any kind of disaster, the whole system will fail, and valuable data will be irrevocably lost. So, it is strongly recommended that you back up the following:

- InTrust Servers
- Configuration Database
- Repository

Generally, Audit database failure is not as critical as other components' failures, because typical workflow presumes that data is collected to repository. Repository backup will help to restore your Audit database: after you recover the repository, you can easily import the necessary events into the database. However, it is recommended that you periodically back up your Audit database and other InTrust components, as described in this guide.

Backup Procedures for InTrust

To minimize the risk of irrevocable data loss, it is strongly recommended that you perform backup procedures for your InTrust components, as follows:

- InTrust Servers: either weekly, or after new agents are added.
- Configuration database: always after any configuration changes; periodically to take into account newly installed agents (daily backup recommended). Alternatively, set up configuration database replication, as described in Replication of the InTrust Configuration Database. This lets you ensure InTrust configuration consistency across the enterprise and increase you InTrust organization's fault tolerance.
- Repository: after each gathering process, i.e. depending on gathering process schedule; at least daily backup recommended.
- Audit database: depending on gathering process schedule (frequency), daily backup recommended.
- Alert database: daily backup recommended.
- InTrust agents: recommended—two times a week.

InTrust provides InTrust Server failover capabilities, which allow for automatic operation switching. It is recommended to activate this feature, as follows:

1. Configure two InTrust Servers in your InTrust organization:
    - A production InTrust Server that performs gathering and real-time monitoring
    - A standby InTrust Server that will take over the operation if a production Server goes down.
2. Create an InTrust site containing the standby InTrust Server, and specify this server name when prompted for InTrust Server responsible for processing the site.
3. To monitor for the state of production InTrust Server, you need to enable the “InTrust server is down” monitoring rule (located in **InTrust Internal Events | InTrust server failover** rule group) on the standby server, and activate the response action (failover script execution) of this rule.
4. When configuring this rule, select to perform matching on server side. Also, you can specify:
    - Which InTrust Servers to monitor
    - How long to wait for response from a monitored server before it is considered to be down
5. Create and activate a monitoring policy involving this rule and the InTrust site created on step 2.

If the production InTrust Server failure occurs, the standby InTrust Server takes over the sites and tasks processed by InTrust server that went down.

CAUTION: **To ensure the availability and integrity of InTrust databases and repositories, it is recommended to locate them separately from the InTrust Servers. This will help minimize the risk of their failure if any of the InTrust servers go down.**

If your agents are planned to be installed manually (for example, automatic agent install is not allowed by your organization's policies), then you should establish agent-server communication for both the production and standby InTrust servers when you install and configure the agents. This will allow agents to connect to a standby server if a failover occurs. (For details, refer to Installing Agents Manually).

IMPORTANT: InTrust server recovery may be incomplete if the failed server was configured to receive forwarded Syslog messages. In this case, a failover operation can cause your Syslog collections to reference the wrong Syslog-receiving InTrust servers. If this happens, open the properties of the affected Syslog collections in InTrust Deployment Manager and select the right Syslog-receiving servers for them.

How to Recover Your InTrust

The following topics give you an idea of the problems which may occur due to a disaster, how they can be solved if you have properly backed up your data, and what if you have not.

InTrust Server Recovery

InTrust Server and Its Temporary Files Corrupted due to Disk Failure

Backup Copy	Solution
Disk backup available	Restore InTrust Server and temporary files to the location where they resided.
No backup	Use InTrust failover capability to switch to other InTrust server in your organization. For that, you should enable the “InTrust server is down” real-time monitoring rule (from the “InTrust server failover” rule group) on the standby InTrust server to monitor for current InTrust server status: 1. On the **General** tab of the rule’s Properties dialog, make sure the rule is enabled. 2. On the **Response Actions** tab, make sure the Failover script execution is selected. Save the settings, and commit the changes.

Backup Copy	Solution
	If a failure occurs, you will get a notification, and standby server will take over the sites and tasks processed by InTrust server that went down. You can perform a failover manually by launching Server Switching Wizard: 1. In InTrust Manager, select **Configuration | InTrust Servers**, and from your current InTrust server's shortcut menu, select **Failover | Switch**. Follow the steps of the wizard: 2. Select the InTrust sites and jobs to be switched. 3. Specify the InTrust server that will take over the operations. 4. Finish the wizard and commit the changes. After restoring the InTrust server, you can roll back this switching session (switch sites and jobs back to the server initially responsible for their processing): 1. Start the Rollback Wizard by selecting **Failover | Roll Back** from the restored server's shortcut menu, and select the session to roll back. 2. Commit the changes after finishing the wizard.

Notes and Caveats

- If you are using role-based administration in your InTrust deployment, consider that to run Server Switching wizard, a user must have **Modify** permission for switched sites and jobs (their nodes in InTrust Manager), and for the InTrust Server node (the one you are switching from)
- By default, passwords for agent-server connection expire in three days after they were set. Thus, if you make a daily backup of InTrust program folder, and you restore it on the new server within 3 days timeframe, the agents should be still able to connect to server. Agent password expiration policy can be adjusted in the configuration database.
- If an InTrust Server that went down was hosting any Data Stores used by the jobs which were running at that moment, then such jobs will fail, and you will have to create them anew. For example, if a gathering job was using an Audit database located on the failed server, it has to be created anew.

System Disk Failure InTrust Server Computer

Backup Copy	Solution
Disk backup available	Restore files from backup.
No backup	Use InTrust failover capabilities, as described above.

InTrust Server IP Address Changed

Details: After the server is restarted, connection with the agents is lost.

Agents	Solution
No agents installed on the computers over the firewall.	• If an agent had been installed automatically, then it is recovered, and agent-server connection is re-established automatically after the heartbeat interval, or when gathering process starts. • If an agent had been installed manually, and agent-server connection had been also established manually, then it is re-established automatically after the heartbeat interval, or after the gathering process starts (it is assumed that gathering is performed using agents). However, make sure the account (under which the InTrust server runs) can access the target computers—otherwise, you need to establish agent–server connection manually. For details, see Installing Agents Manually.
Several agents installed on the computers over the firewall.	Agent-server connection for these agents must be established manually. For more details, see Installing Agents Manually.

CAUTION: After recovery, an agent tries to connect to InTrust server whose name (NetBIOS name, FQDN, or IP address) was provided to this agent during the installation procedures (that is, when the server was registered on agent).

If you have specified the FQDN (recommended), then the agent will search for the InTrust server using this name, and connect to the server automatically.

However, if the server's IP address had been specified (for example, in case of DMZ, or some DNS problems) that was later changed, you should re-register that server on the agent, as described in the Establishing a Connection with the Server topic in Installing Agents Manually.

InTrust Agent Recovery

Agent Failure (Target Computer is Over Firewall)

Backup Copy	Solution
Target computer backup available	Restore target computer from the backup. Agent will be recovered and restarted automatically. You should manually establish agent-server connection, as described in Installing Agents Manually.
No backup	Recover the target computer and re-install the agent. For details, see the Deploying Agents topic in the Deployment Guide.

Agent Failure (Target Computer is Not Over Firewall)

Backup Copy	Solution
Target computer backup available	Recover target computer from the backup. After that: • If agent was installed automatically, then it will be recovered, and agent-server connection will be re-established automatically after the heartbeat interval, or when gathering process starts. • Otherwise, agent-server connection must be re-established manually, as described in the Establishing a Connection with the Server topic in Installing Agents Manually.
No backup	Recover a target computer with the same name. • If installed automatically, an agent will be recovered and re-connected with the server when gathering process starts, or when site computers are enumerated for the monitoring. • If installed manually, an agent should be re-installed and re-connected manually.

Configuration Database Recovery

Configuration Database Failure

Backup Copy	Solution
Database backup available	Restore the configuration database from the backup and apply changes (if any) made after the backup; restart each InTrust Server.
No backup	There is no way to restore configuration database. All configuration data is lost. You must re-deploy InTrust Organization anew (create a new Configuration database, re-install all InTrust servers and configure all components).

Using the adccfgdb.exe Utility

The **adccfgdb.exe** utility is included in the InTrust Resource Kit to help you switch the configuration database for the InTrust server (on which you run the tool) from one SQL server to another. You can launch the utility, for example, if your original SQL server with the InTrust configuration database went down because of the system disk failure (but the database is safe), or to switch to another SQL server whenever needed.

NOTE: You can also use this utility to set new credentials for accessing your existing configuration database. For details about utility usage, run **adccfgdb.exe** without any arguments.

Use the utility as follows:

1. Stop the Quest InTrust Server and Quest InTrust Real-Time Monitoring Server services.
2. If SQL server is running and you just need to switch the InTrust configuration database to another SQL server, then detach this database on the current server, and attach it on the new server.
3. If SQL server went down because of the system disk failure, then move all configuration database files to another SQL server and attach this database on that server.
4. Launch the adccfgdb.exe utility on the InTrust server, as follows:
   ```
   adccfgdb.exe [/auth {SQL|NT}] [/server <sqlname>] [/database <dbname>] [/user <username>] [/password <pwd>|{*}]
   ```
   where
   /auth {SQL|NT}—authentication method to be used when connecting to the database
   /server <sqlname>—name of the SQL Server where the InTrust configuration database will reside
   /database <dbname>—database name
   /user <username>—user name to be used in SQL authentication mode
   /password <pwd> |{*}—password to be used in SQL authentication mode, or asterisk if the password will be supplied interactively

After the utility has finished running, open the properties of the configuration database available in **InTrust Manager | Configuration | Data Stores**, and specify the new configuration database location and/or access credentials.

CAUTION: **The account you specify must be granted the same access rights on the SQL server and configuration database as before switching.**

Audit Database Recovery

Audit Database Failure

Backup Copy	Solution
DB backup available	Restore Audit database from the backup.
No backup	To avoid re-configuring your gathering jobs, create the new Audit database in the following way: 1. In InTrust Manager, select **Configuration | Data Stores | Databases**, and open your Audit database properties. Find out the database name, location, and access credentials. 2. On the SQL Server specified as database location, create a new Audit database with the same name and access credentials using SQL Server tools. Verify connection settings by connecting to this database with the specified credentials. Data can be imported to the new database from your repository.

.

Alert Database Recovery

Alert Database Failure

Backup Copy	Solution
Database backup available	Restore Alert database from the backup.
No backup	All alert data is lost. To create a new Alert database: 1. In InTrust Manager, select **Configuration | Data Stores | Databases**, and open your Alert database properties. Find out the database name, location, and access credentials. 2. On the SQL Server specified as database location, create a new Alert database with the same name and access credentials. Make sure the Monitoring Console web application account can access the new database. 3. After you create a new Alert database, open the Monitoring Console Administration page (for example, from the Start menu), and on the **Database** tab check the credentials for database access.

Repository Recovery

Repository Failure

Backup Copy	Solution
Repository backup available	Restore the repository from the backup; in **InTrust Manager | Configuration |Data Stores | Repositories**, modify the UNC path in the properties of the repository object so that it refers to recovered repository.
No backup	Repository data is lost. 1 In InTrust Manager, select **Configuration | Data Stores | Repositories**, and open your the properties of your repository. Find out the repository name and location. In the file system, create a new repository with the same name and location. 2 Alternatively, a new repository can be created automatically (in the location specified in the repository properties) when a gathering job starts.

Monitoring Console Recovery

InTrust Monitoring Console Failure

Backup Copy	Solution
InTrust Configuration Database operates normally, or has been restored from the backup	Reinstall Monitoring Console.
No backup of InTrust Configuration Database	For details, see Configuration Database Recovery. After you have recovered the configuration database, reinstall Monitoring Console and reconfigure all profiles.

InTrust Manager Recovery

InTrust Manager Corrupted due to Disk Failure

Backup Copy	Solution
Disk backup available	Restore InTrust Manager from the backup.
No disk backup	Reinstall InTrust Manager.

Knowledge Portal Recovery

Knowledge Portal Web Application Fails

Reinstall Knowledge Portal component. Report Packs will be available for use without special recovery measures.

SQL Server Reporting Services Failure

Backup Copy	Solution
Reporting Services backup available	Restore Reporting Services from backup. Backup and recovery procedures are described in Backup and Restore Operations for a Reporting Services Installation. Report Pack will be available for use without special recovery measures.
No backup	Install Reporting Services anew; Report Packs must be reinstalled.

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