InTrust® 10.2

Replication of the InTrust Configuration Database
Replication of the InTrust configuration database involves keeping a regularly synchronized replica of the database on additional SQL servers.

InTrust sessions are not replicated.

This gives you the following benefits:

- **InTrust configuration consistency across the enterprise**
  In enterprises that operate globally, InTrust deployments in all the locations cannot use the same configuration database. A partial solution is to have multiple configurations, but it is better to keep a replica of the master configuration database in each location.

- **Increased fault tolerance**
  In the event that the SQL server with your configuration database fails, your configuration is not lost. Furthermore, if InTrust is configured to automatically switch databases in such circumstances, then the impact of the failure is minimized.

This document outlines two possible scenarios, which illustrate these points:

- WAN Link Scenario
- SQL Server Failover Scenario

The configuration described is supported for SQL Server 2005 or higher.
Before You Set Up Replication

Prepare InTrust for Replication

Make sure to create an up-to-date backup of your InTrust configuration database before you start configuring its replication.

Prepare SQL Servers for Replication

1. Verify that the name of each SQL Server participating in the replication matches the network name of its local machine.

   To check whether you have a mismatch between your SQL Server name and the computer's name, compare the values from the statements that follow. If the values do not match or if @@SERVERNAME is NULL, you need to rename your SQL Server.

   To get the current SQL Server name/instance name, use the following query:

   ```sql
   SELECT @@SERVERNAME
   ```

   To get the current machine name and instance name, use the following query:

   ```sql
   SELECT SERVERPROPERTY('MachineName'), SERVERPROPERTY('InstanceName')
   ```

   For more information, see http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B303774.

2. Make sure that the Microsoft SQL Server version on the Subscriber side is less than or equal to that of the Publisher. To get SQL Server version information, use the following query:

   ```sql
   SELECT SERVERPROPERTY('productversion')
   ```

3. Create a new empty InTrust configuration database on the Subscriber SQL Server using the following query:

   ```sql
   CREATE DATABASE <new database name>
   ```

   If you are going to implement the SQL Server failover scenario, make sure that a database name and access credentials are the same for both the main and the backup configuration database.

4. Set up rights and permissions for accounts to be used by the Snapshot Agent and Merge Agent as described in the Permissions Required by Agents section later in this document.
Setting Up Replication

1. Configure a distribution for the SQL Server that will be publishing your InTrust configuration database (Publisher). For more information, see the To configure a distribution procedure in the Technical Details and Procedures section later in this document.

2. Create a publication for the InTrust configuration database on the Publisher SQL Server. For more information, see the To create a publication in the Technical Details and Procedures section later in this document.

3. On the SQL Server that hosts the new InTrust configuration database, create a subscription for this publication, as described in the To create a subscription procedure in the Technical Details and Procedures section later in this document.

4. Wait for initial synchronization to complete successfully. To monitor the synchronization status, right-click the name of the subscription you have created and select View Synchronization Status from the shortcut menu to see a message in the Status pane reading:

   Waiting 60 second(s) before polling for further changes.

5. Connect to the Subscriber SQL Server (the one where you have created the subscription on the previous step) using credentials with the db_owner role for the new InTrust configuration database. Run the configdb.sql script (find it in the <InTrust_DVD>\Scripts\Database Scripts folder) on that database. You may receive some errors while the script is running, such as:

   • "Updating columns with the rowguidcol property is not allowed."
   • "GETMAXVERSION: The parameter 'lineage' is not valid."
   • "The statement has been terminated."

   These errors can be safely ignored.

Technical Details and Procedures

To configure a distribution

1. Connect to the Publisher SQL Server (the one that hosts your existing InTrust configuration database) with Microsoft SQL Server Management Studio, and expand the node of that server.

2. Right-click the Replication folder and then click Configure Distribution.

3. Follow the Configuration Wizard steps.
When you configure the Distributor, you specify the following:

- A snapshot folder, which is used, by default, for all Publishers that use this Distributor. Ensure that this folder is already shared and has the appropriate permissions set.
- A name and file location for the distribution database. The distribution database cannot be renamed after it is created. To use a different name for the database, you must disable distribution and reconfigure it.
- Any Publishers authorized to use the Distributor. If you specify Publishers other than the instance on which the Distributor runs, you must also specify a password for the connections the Publishers make to the remote Distributor.

To create a publication

1. Connect to the Publisher SQL Server with Microsoft SQL Server Management Studio using credentials with the sysadmin role for that SQL Server.
2. On the InTrust configuration database to be published, execute the AdcCfgPublication.sql script with no parameters.

   When you run the script on SQL Server 2008, you may get warnings like the following:

   Warning: Values of some of the flags specified in the 'schema_option' property are not compatible with the publication's compatibility level. The modified schema_option value of '0x000000b230034fd0' will be used instead.

   These warnings can be safely ignored.
3. Verify that a publication named AdcCfgPublication has been created on the Publisher SQL Server for that database.
4. On the Publication Access page of the publication Properties dialog, add the account you plan to use for the Merge Agent.
5. On the Agent Security page, create a Snapshot Agent (if not yet created). Verify that the account specified for this agent meets the requirements stated in the Permissions Required by Agents section later in this document.
6. Verify that the snapshot of the published database is created. To do so, right-click AdcCfgPublication and select View Snapshot Agent Status in the shortcut menu. If the last message there is “The agent has never been run.”, start the agent by clicking the Start button and wait for a message like: [100%] A snapshot of 120 article(s) was generated.

To create a subscription

1. Connect to the Subscriber SQL Server with Microsoft SQL Server Management Studio using credentials with the sysadmin role for that SQL Server.
2. Expand the Replication node under the node of Subscriber server, right-click Local Subscriptions and then select New Subscription.
3. Follow the steps of the Configuration Wizard:
   - Select the Publisher and the publication you have created (see the To create a publication procedure earlier in this document).
   - Select Push subscription.
   - Select the new InTrust configuration database you have created as a target database for the replication.
• Specify an account that the Merge Agent will use to connect to the Publisher and Subscriber (see the Permissions Required by Agents section below).
• Select Run continuously for the synchronization schedule.
• Unless you have your reasons for not doing so, select the option to initialize the subscription immediately.
• Select Client as the subscription type.

If you have more than one subscriber, you should create a database snapshot before adding each subsequent subscriber. If any changes occur in the database since the latest snapshot, these changes will be lost after the addition of a new subscriber.

**Permissions Required by Agents**

**Snapshot Agent**

• The Windows account under which the agent runs is used when making connections to the Distributor. This account must be a member of the db_owner fixed database role in the distribution database and has write permissions on the snapshot share.
• The account used to connect to the Publisher must at minimum be a member of the db_owner fixed database role in the publication database.

**Merge Agent for a Push Subscription**

The Windows account under which the agent runs is used when making connections to the Publisher and Distributor. This account must:

• At minimum be a member of the db_owner fixed database role in the distribution database
• Be a member of the PAL
• Be a login associated with a user in the publication database
• Have read permissions on the snapshot share

The account used to connect to the Subscriber must at minimum be a member of the db_owner fixed database role in the subscription database.

**Merge Agent for a Pull Subscription**

The Windows account under which the agent runs is used when making connections to the Subscriber. This account must at minimum be a member of the db_owner fixed database role in the subscription database.

The account used to connect to the Publisher and Distributor must:

• Be a member of the PAL
• Be a login associated with a user in the publication database
• Be a login associated with a user in the distribution database (the user can be the Guest user)
• Have read permissions on the snapshot share
Scenarios

WAN Link Scenario

Before you implement the WAN Link scenario, you have to set up a replication as described earlier in this document.

As mentioned in the InTrust Best Practices document, each InTrust server must have a fast and reliable connection with the SQL server where InTrust configuration database resides. This solution lets you work with geographically dispersed InTrust Servers that are connected over a slow WAN link.

The configuration shown below has two InTrust Servers and two identical SQL Server computers with replicas of the InTrust configuration database that are synchronized to maintain consistency.

![Diagram showing two InTrust Servers and two SQL Servers with database replication](image-url)
Making InTrust Work with the Replicated Database

Install new InTrust Servers in the usual way. When prompted for location and name of the configuration database to use, specify the Subscriber SQL Server and the name of the new (replicated) database. You may receive some errors such as:

```
Cannot update the InTrust configuration database. Reason:
GETMAXVERSION: The parameter 'lineage' is not valid. The statement has been terminated. The statement has been terminated.
```

These errors are safe to ignore. Click Ignore and continue with the setup procedure.

SQL Server Failover Scenario

Before you implement the scenario, you have to set up a replication as described earlier in this document.

A common and often inexpensive approach to recovery after failure is to maintain a standby system to assume the production workload if the production system failure occurs. A typical configuration has one InTrust Server and two identical SQL Server computers with a copy of the InTrust configuration database. If the InTrust configuration database becomes unavailable, the InTrust Server can switch to the other SQL Server, as shown in the picture below:
InTrust provides the **Configuration DB is down** rule that is matched when the InTrust configuration database becomes unavailable to the InTrust server. This is indicated by **Event ID 6565** in the InTrust Server log. The rule has the **Switch Configuration DB** response action, which puts a script into a temporary folder and runs it. The script switches the InTrust server to a replica of the configuration database and restarts InTrust.

- For the response action to work correctly, the database name and access credentials must be the same for both the main and the backup configuration database.
- The rule, response action and script files used in the following procedure are located in the **Scripts\Database Replication** folder in your InTrust distribution.

### Preparing InTrust for a Failover Scenario

1. Run InTrust Manager.
2. Import the **Configuration DB is down** rule under **Real-Time Monitoring | Rules | InTrust Internal Events | InTrust Server Failover**.
3. Import the **Switch Configuration DB** response action under **Configuration | Advanced | Scripts** using the **InTrustPDOImport.exe** command-line utility, which is available in the ADC Server Resource Kit, in the `<InTrust_installation_folder>\InTrust\Server\ADC\SupportTools` folder.
4. Select a site from the list of existing InTrust sites or create a new one which is populated with InTrust Servers of your InTrust Organization.
5. Create a monitoring policy that includes the InTrust site that was specified on the previous step and the **Configuration DB is down** rule.
6. Right-click the **Configuration DB is down** rule and select **Properties**.
7. Click the **Response Actions** tab and make sure that the **Execute script** option is selected. Check that the following script parameters are specified correctly; otherwise, the default values will be applied:
   - **Backup configuration DB Server**
     Specify the `<SQL server name>\<instance name>` that hosts the backup configuration database. For example, "sqlserver02.domain.corp".
   - **Main Configuration DB Server**
     Specify the `<SQL server name>\<instance name>` that hosts the main configuration database. For example, "sqlserver01.domain.corp".
   - **Switch Once**
     This parameter can be set to "No" or "Yes". If InTrust is already working with a backup configuration database and the database is failed, "No" means that it will switch back to the main configuration database, and "Yes" means that it will not switch.
About Quest Software, Inc.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier. Visit www.quest.com for more information.

Contacting Quest Software

Phone 949.754.8000 (United States and Canada)
Email info@quest.com
Mail Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA
Web site www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a Quest product and have a valid maintenance contract. Quest Support provides unlimited 24x7 access to SupportLink, our self-service portal. Visit SupportLink at http://support.quest.com/

From SupportLink, you can do the following:

- Retrieve thousands of solutions from our online Knowledgebase
- Download the latest releases and service packs
- Create, update and review Support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: http://support.quest.com.