Quest® InTrust 11.6.0

Replication of the InTrust Configuration Database

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 Replication of the InTrust Configuration Database
Updated - November 2023
Version - 11.6.0

Contents

Benefits of Configuration Database Replication

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

NOTE: 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 later.

Before You Set Up Replication

Prepare InTrust for Replication

Make sure you have 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.

NOTE: 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:

```
SELECT @@SERVERNAME
```

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

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

For more information, see the Rename a Computer that Hosts a Stand-Alone Instance of SQL Server article.

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:
   `SELECT SERVERPROPERTY('productversion')`
3. Create a new empty InTrust configuration database on the Subscriber SQL server using the following query:
   `CREATE DATABASE <new database name>`

NOTE: 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 topic.

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 topic.
2. Create a publication for the InTrust configuration database on the Publisher SQL Server. For more information, see the *To create a publication* procedure in the Technical Details and Procedures topic.
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 topic.
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 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 **Scripts\Database Scripts** folder in your InTrust distribution) 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.

Using the Configuration Database Replica

Before you can use the database replica as a full-featured InTrust configuration database, you need to perform an additional initialization step. You can do it in one of two ways:

- Install a new instance of InTrust Server that uses the replica as the configuration database.
  If you were planning to deploy new InTrust servers for this configuration replica anyway, this is a good time to do so. During InTrust Server installation, the database will be initialized automatically.
- Run the special-purpose **configdb.sql** script on the database to perform the initialization.
  This script is located in the **Scripts\Database Scripts** folder in your InTrust distribution. Use the script if you have no plans to deploy new InTrust servers that use the configuration replica.

Technical Details and Procedures

To configure a distribution

1. In Microsoft SQL Server Management Studio, connect to the SQL server that you want to configure as the Distributor (if unsure, use the Publisher server that publishes your InTrust configuration database), 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 that the Publishers make to the remote Distributor.

In addition, you need to make sure the "Agent XPs" stored procedure is enabled. Otherwise, you will get an error like the following:

```
SQL Server blocked access to procedure 'dbo.sp_set_sqlagent_properties' of component
'Agent XPs' because this component is turned off as part of the security
configuration for this server.
```

To enable this stored procedure, run the following SQL query:

```
sp_configure
sp_configure ‘show advanced options’,1
reconfigure
sp_configure 'Agent XPs',1
reconfigure
```

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.

NOTE: When you run the script, 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 topic.
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 such as "[100%] A snapshot of 146 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 topic).
    - 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.

NOTE: 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.

Important: After you have created a subscription for a new database, wait until the initial replication between the publisher and subscriber databases completes. After that, you can safely proceed with configuration.

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 have write permissions on the snapshot share.
- The account used to connect to the Publisher must at least 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 least 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 for connection to the Subscriber must at least 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 least be a member of the **db_owner fixed database** role in the subscription database.

The account used for connection 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

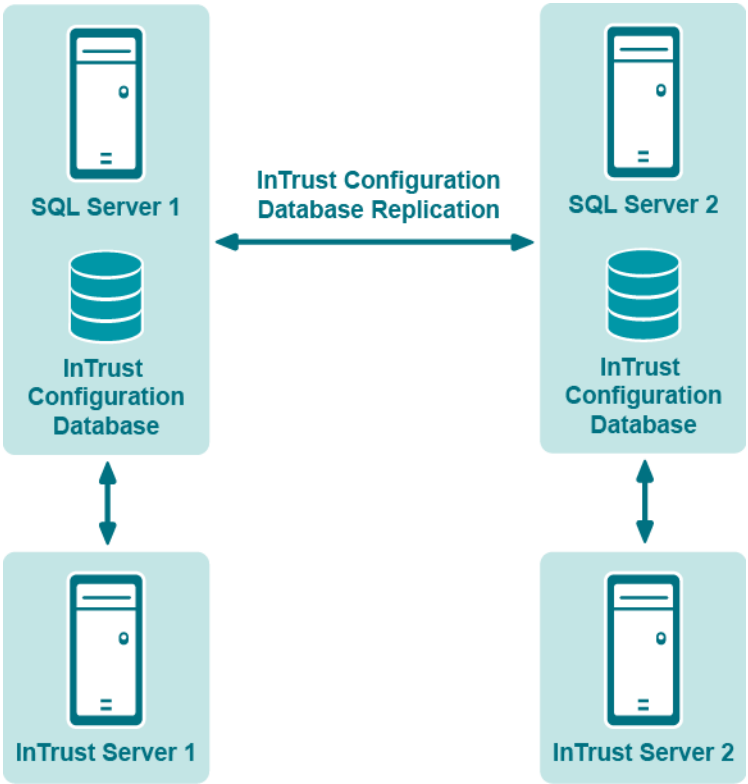
Scenarios

WAN Link Scenario

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

Each InTrust server must have a fast and reliable connection with the SQL server where the 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.



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.

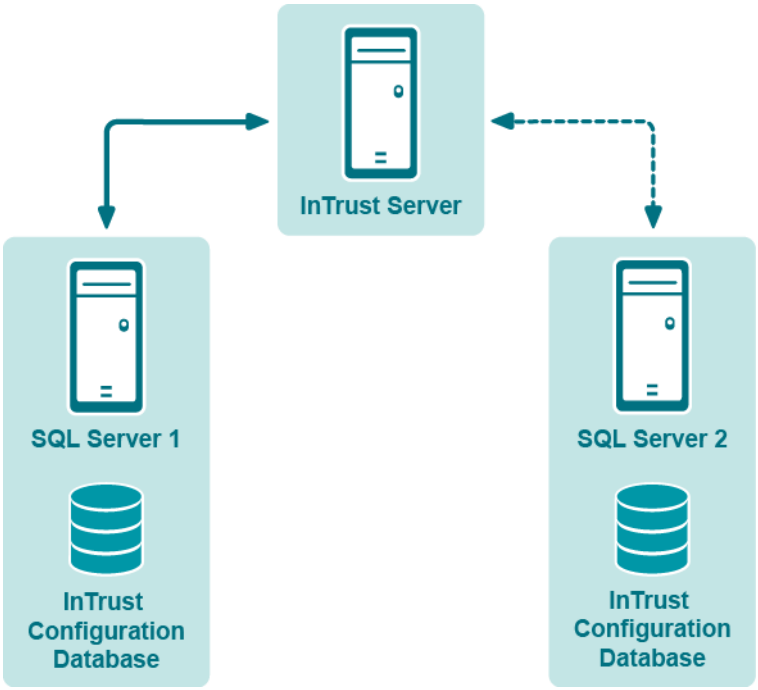
Upgrading InTrust Servers in WAN Link Scenario

Upgrading InTrust organizations with the WAN link scenario implemented is specifically described in the Upgrade Guide.

SQL Server Failover Scenario

Before you implement the scenario, make sure you have made the configuration changes described in Setting Up Replication.

A common and often inexpensive approach to recovery after failure is to maintain a standby system to assume the production workload if a 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, which 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.

NOTE:

- 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 the 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 has failed, "No" means that it will switch back to the main configuration database, and "Yes" means that it will not switch.

SQL Server Failover for Multiple InTrust Servers

If multiple InTrust servers share a configuration database (or a replica of a configuration database), then a few additional steps are necessary to make them switch to a standby configuration database. You can do this in one of two ways:

- Duplicate the failover configuration for each server
- Use a shared failover configuration

Duplicating the Configuration

Perform steps 1 to 3 from the Preparing InTrust for a Failover Scenario topic.

Then, for each of the InTrust servers, do the following:

1. Create a site that is owned by the InTrust server, and include the server itself in this site. Name the site so that it indicates the InTrust server that uses it.

2. Make a copy of the **Configuration DB is down** rule, and append the name of the InTrust server to its name, so that you can easily tell the similar rules apart.
3. Create a monitoring policy that includes the InTrust site from step 1 and the rule from step 2. Give the policy a matching name.
4. In the properties of the duplicated rule, configure the response action as explained in the Preparing InTrust for a Failover Scenario topic.

When you have done this for all InTrust servers that participate in the failover configuration, commit your changes. Now, if the main configuration database goes offline, each of the servers will independently switch to the standby database.

Using a Shared Configuration

A shared configuration is slightly easier to set up and modify.

Perform steps 1 to 3 from the Preparing InTrust for a Failover Scenario topic, and then do the following:

1. Create a site that includes all of the InTrust servers you need.
2. Right-click the site and select **Install Agents**. Note that this does not install any additional software on the InTrust servers—it just enables the hidden agent-specific functionality that is not normally used on a server.
3. Create a monitoring policy that includes the new InTrust site and the **Configuration DB is down** rule.
4. In the properties of the rule, configure the parameters of the response action as explained in the Preparing InTrust for a Failover Scenario topic.
5. In the properties of the response action, on the **General** tab, select the **Agent** option.
6. Commit your changes.

Now, if the main configuration database goes offline, each of the servers will independently switch to the standby database.

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