Nimsoft options for routing messages (QoS/Alarms) between hubs

Document updated 10/28/2011
This document covers the following options:

A. attach and get queues
B. post queues
C. nas replication

The table below describes different options for use in deciding which approach to use.

<table>
<thead>
<tr>
<th>Option</th>
<th>QoS Fwd</th>
<th>Alarm Fwd</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>attach/get queues (hub)</td>
<td>Yes</td>
<td>Yes</td>
<td>• Confirmation of delivery (spools messages) if hub is down.</td>
<td>• Queues limited by Winsock limit on Windows machines. The Windows event mechanism can only wait on 64 event objects at a time. If there are ~64 hub subscribers, messages may become stuck in the queue.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Internal alarm generated when hub connection is lost. Alarm generated when get queue connection cannot be established.</td>
<td>• attach/get queues are only allowed between Hubs within the same Domain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• More manageable than post queues.</td>
<td></td>
</tr>
<tr>
<td>post queues (hub)</td>
<td>Yes</td>
<td>Yes</td>
<td>• Light-weight, less message/network traffic.</td>
<td>• post queues do not guarantee delivery/cannot confirm receipt of message.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No alarm when hub is lost.</td>
<td>• If the connection between 2 hubs is down, the messages are queued in the post queue on the sending machine. Once the link is re-established, the messages are sent to the destination hub.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• post queue(s) can send data across domains (to a different NMS Domain.). You can use post queues between hubs in different domains to send messages cross-domain in a non-tunneled environment but you have to use Static Hubs between domains.</td>
<td>• If there is no attach queue on the destination hub, the messages would be lost.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Simple, not manageable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Recommended for use with audit messages: Use post queues on the remote hubs to send all audit messages to the main hub by creating a post queue with a subject of ‘audit.’ Point the post queue to the main hub. - allows you to view all audit activity from the main hub.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Best practice for post queues is to create one post queue for QoS and one for Alarms.</td>
</tr>
<tr>
<td>nas replication</td>
<td>No</td>
<td>Yes</td>
<td>• Avoids the limitation of 64 max subscribers on Windows platform.</td>
<td>• Alarms Only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Scalability/reliability needs further</td>
</tr>
</tbody>
</table>
A. **attach and get queues (hubs/tunnels)**

Once a new hub/tunnel is active and available you need to add the QoS and Alarm queues so your remote hub/customer’s client can send QoS/Alarms to your primary server Hub for archiving and notification.

Essentially you create the “attach” queues on the remote hub and the “get” queues on the primary Hub via the “Queues” tab.

1. You will need to access the remote hub/customers Hub probe to create “Attach” queues.

   This is done by selecting the Hub probe and the “Queues” tab.

   ![Hub_probe_and_queues_table](image)

   **Important:** Do **NOT** delete the automatically configured nas and data_engine Message Queues pictured above.

   **Attach** queue, creates a permanent queue for any client to attach to.

   By selecting the “New” button you can create a new queue.
You will need to create an “attach” queue for the “alarm” data.

Once created you can now exit out of the remote hub/customer’s hub probe.

Note that you could create a single queue for both QoS and alarms e.g., “QOS_MESSAGE,QOS_DEFINITION,alarm” if you are worried about the Windows limit. The down side is that alarms could get slowed down if there are a lot of QOS messages. However this would be rare. You now need to create the coinciding queues on the primary Server Hub that “get” the queues.
In this interface you will use the drop down selection to add the “Address:” field and select the proper Nimsoft address/hostname/IP address of the customers hub and select the “Queue:” that will be gathered.

Once done adding the two “get” queues (for QoS and alarms), Save your changes to the hub probe.

Don’t modify Bulk Size unless instructed by a Nimsoft Support engineer. Leave as default.

**B. Post queues**

To create a post queue, select the Queue’s tab at the top of the window, and click the New button to set up a new queue. Example below…

Click Ok, to save the Queue, and OK to save the hub configuration. When prompted to restart the hub, click Yes.

**C. nas Replication (nas probe)**
If you would like to use NAS replication instead of attach/get queues, the alarms will not go through the pre-processing rules that are set up on the primary NAS. You will either have to have two locations for filters, or go back to using get and attach queues.

**Forwarding & Replication**

In the NAS probe under “Forwarding and Replication” you may define other alarm servers with which you want to exchange alarms and/or scripts. Right-clicking in the list lets you add, edit or delete such connections.

Checking the “Relay forwarded alarm events” option, alarms received from another remote NAS will be forwarded, e.g., to the NAS on another hub higher in the hub tier, or the primary hub.

Note: When setting up forwarding and replication and making configuration changes on more than one NAS, you should first open and edit the GUI for one NAS, apply the changes and then exit the GUI. Then you should open and edit the GUI for the next NAS, etc. Otherwise the settings may not be saved correctly.

**Example:** NAS B receives alarms from NAS A, and NAS B forwards alarms to NAS C:

The alarms NAS B receives from NAS A will be forwarded to NAS C only if the “Relay forwarded alarm events” option is set on NAS B.

You can choose to do unidirectional (one-way from one hub to another) or bi-directional replication (two-way between two hubs). Both of these types of replication will create a replication profile on the corresponding NAS. In the case of unidirectional it will set the non-forwarding NAS to send only updates to the alarm (Event Responder).

**Key Options for Forwarding:**

**All alarm events in both directions**
Clicking this option, all alarm events will sent to and received from the NAS selected as destination alarm server. (bi-directional replication)

**All events to destination**
Clicking this option, all alarm events will be sent to the NAS selected as destination alarm server. (uni-directional replication)
As event responder
This option allows the NAS selected as destination alarm server to act as an event responder, enabled to close and assign alarm messages from the NAS that is forwarding the alarm messages. If setting up a queue as “All events to one direction” on NAS A, the queue will appear as “As event responder” on NAS B.

Replication options for destination

Script replication
Select this option if you want the scripts available on the NAS to also be available for the destination NAS defined.

- None means not available for the destination alarm server defined.
- Private means that scripts will be available on the destination NAS defined, but it cannot be modified there (no write access).
- Shared means that scripts will be available on the destination NAS defined, in the same script structure as the source NAS, and it is possible to modify the script. Changes will be mirrored between the two NAS’s.

NOTE if sharing scripts with a destination NAS:
If modifying a shared script on the destination NAS, you MUST create a folder where you save the modified script. Otherwise it will be overwritten if the script is modified on the origin NAS (the NAS where the script was created).

Configuration replication (AO Profiles)
Select this option if you want the configuration settings (e.g., Auto-Operator profiles) available on the NAS, also be available for the destination alarm server defined.

None means not available for the destination alarm server defined.

Example:
- Set Configuration to ‘Private’ in the nas replication configuration.
Private means that the NAS configuration file WILL be available on the destination NAS defined.

Private means that the NAS configuration file will be available on the destination NAS defined.

The file will be located under the directory:

   ..\Nimsoft\probes\service\nas\replication\config<name of the replicated nas server>\nas.cfg

IMPORTANT: If you want to use this configuration file on the destination server, you MUST manually copy it to:

   ..\Nimsoft\probes\service\nas\nas.cfg

Note:
When re-activating replication between two NAS’s, you should manually delete all alarms on the ‘receiving’ NAS that are received from the ‘sending’ NAS.
Replication - Technical Details

This module is responsible for replicating alarm data, script files and configuration data to its replicating endpoints by export and import mechanisms. The replication data is stored in an outgoing queue in the replication directory structure. Each queue is a SQLite database containing two tables, REPL_CONFIG and REPL_QUEUE. The current replication configuration is serialized and stored in the REPL_CONFIG table. Changes to the configuration will result in a full cold-start of the queue i.e the queue file is removed.

Events will be extracted from the internal bus and stored into the various queues along with files and configuration data. Alarms that have a complete transaction (new + close) in the queue will not be translated to console events. The queues will be bulk exported through the NimBUS request repl_queue_post. The bulk size is configurable, and is default 2000 queue items. The bulk data is stored on the remote NAS as replication/*.import file.

A separate ‘replication importer’ thread is started and will attempt to read the import file from all configured alarm servers in the replication schema on interval and will process the whole import file as quickly as possible. When the nas receives a bunch of messages from a nas that’s replicating to it, it writes it to the import file. Then, the import file is read by the importer, which stuffs the alarms into the replication database (database.db) then deletes the import file.

How to setup ‘selective’ forwarding between nas probes

NAS replication will place alarms into the receiving nas after pre-processing takes place. This prevents forwarding of forwarded alarms by the receiving nas. This section discusses one way to selectively forward alarms between nas probes.

In this scenario we will use an Auto Operator profile, on the remote/secondary nas, to repost alarms to forward. The reposting will be done with a Subject of forward. A post queue on the secondary hub will then send those Subjects to the primary hub.

The primary hub is a modified nas queue that listens to both alarms and forward. The primary nas is configured for both alarm and forward Subjects. When an alarm reaches the nas queue with the subject of ‘alarm’ or ‘forward’ the nas probe will take the alarm from the nas queue and process it using normal Auto Operator rules.

Example:

On the remote/secondary nas, create an Auto Operator profile to repost alarms using the Subject of ‘forward’
Create a post queue from the secondary hub to the primary hub.

Modify the nas queue on the primary hub, to subscribe to both ‘alarm’ and ‘forward’ Subjects.
Modify the nas configuration on the primary hub using Raw Configure, to ‘listen’ for both ‘alarm’ and ‘forward’ Subjects.

Create your normal Auto Operator profiles in the primary nas to manage alarms.

**Hub Queues - Bulk Size**

The parameter defines how many messages that should be transferred simultaneously (in one bulk). The only time you need to change this value from ‘<default>’ is when you see that the queue grows and never
shrinks to zero (see Subscribers Queues on the Status tab). This indicates that the Hub has problems delivering the messages to the target Hub fast enough. The reason for this behavior could be that the number of QoS messages delivered to the Hub from the Robots has increased a lot (See Statistics button on the General tab) or that the latency is too high and slows down the deliveries (See Response Check, right-clicking a Hub in the Hubs list).

Default Bulk size: The hub sends 1 message, and waits for an 'acknowledge' from the peer hub. <num> bulk size defines how many messages are sent in 1 bulk, before an acknowledge (ACK) is received. The <default> bulk size allows the software to determine the best bulk size. A high setting e.g., 50 can actually cause problems with the queue(s) dropping due to large amount of buffering. This is set on the Queues tab, right-click on each queue to edit.

Bulk size was implemented as a way to tune the communication between 2 hubs, especially on networks with high latency (in order to produce the best throughput).

**Nas replication and Max Transfer Blocksize (messages)**

Max. Transfer Blocksize (messages)
This parameter sets the maximum number of messages transferred at each interval. You may select one of the values available or preferably select automatic (default).

The NAS will then attempt to use a blocksize of 10000 messages. If the NAS fails to send so many messages (after 10 attempts), the blocksize will automatically be divided by 10, and the NAS attempts to transfer 1000 messages. If still problems, the blocksize will again be divided by 10 (to 100). This continues until the NAS succeeds to send the current blocksize.

Then the NAS uses this blocksize for 10 intervals, and then increments the blocksize with 100. If this works OK, the blocksize will again be incremented by 100 for the next 10 intervals. This continues until the highest possible blocksize is reached.

Parameters:
replication->num_failures <integer> 20 Before generating alarm.
replication->queue_reconnect <integer> 60 Reconnect freq. in seconds
replication->service_interval <integer> 60 Freq. for checking changes to scripts and configuration.
replication->service_monitor <integer> 900 Repl. queue size monitor.

The alarm is fired after 20 failures, this counter is reset after a good connect.

Note that Default timeout under Advanced->Timeout is 15 seconds.

Miscellaneous: Number of subscribers

There is a central dispatch mechanism for the subscribers where we get increasing dispatch overhead with an increasing numbers of subscribers. There will be a limit for the number of subscribers on Linux too, and our guess is that it is similar to Windows.