

# **AIOps**

## **DX Infrastructure Manager (UIM)**

**Worldwide Support Team**

**High Availability (HA) Guide**

***Updated: January 8, 2020***

*Author: Steve Danseglio*

*Contributors/Reviewers:*

*Jim Christensen, Luc Christian, Kathryn Maguire*

## Table of Contents

<b>BACKGROUND .....</b>	<b>2</b>
<b>HIGH AVAILABILITY USE CASE CONSIDERATIONS .....</b>	<b>2</b>
<b>UIM HIGH AVAILABILITY (HA) .....</b>	<b>3</b>
ENVIRONMENT .....	3
<b>HA SETUP INSTRUCTIONS – SUMMARIZED CHECKLIST .....</b>	<b>4</b>
<b>UIM SECONDARY (HA) HUB .....</b>	<b>4</b>
OPTION 1: MANUAL HA HUB SETUP.....	4
OPTION 2: HA HUB INSTALLATION (VIA UIM SERVER INSTALLER).....	4
<b>SECONDARY (HA) HUB – REQUIRED AND OPTIONAL PROBES .....</b>	<b>6</b>
PROBES TO KEEP ACTIVATED – CHECKLIST.....	9
<b>HA HUB SETUP STEPS.....</b>	<b>9</b>
CONFIGURE DISTRIBUTION SERVER AND LICENSES.....	10
CONFIGURE THE SECONDARY (HA) HUB SO THAT IT CONTAINS THE REQUIRED QUEUES FOR QOS AND ALARMS .....	13
DISABLE NAS NIS BRIDGE.....	15
CONFIGURE NAS ALARM ‘FORWARDING & REPLICATION’ ON PRIMARY & SECONDARY (HA) HUB .....	16
<i>Tips on nas replication and forwarding configuration .....</i>	<i>18</i>
CONFIGURE NAS AUTO-OPERATOR ON THE SECONDARY (HA) HUB .....	18
REQUIRED NAS CONFIGURATION FILE EDITS .....	20
SCRIPTS FOLDER .....	21
<b>HA PROBE CONFIGURATION .....</b>	<b>21</b>
QUEUES TO ENABLE .....	22
PROBES TO ENABLE.....	22
KEY PROBE STARTUP/OPERATIONAL DEPENDENCIES FOR HA .....	23
HA OPTIONS TAB SETTINGS .....	24
<b>HA TESTING .....</b>	<b>24</b>
<b>SECONDARY (HA) HUB POST-FAILOVER .....</b>	<b>26</b>
<b>SECONDARY (HA) HUB PROBE STATUS AFTER FALLBACK .....</b>	<b>26</b>
<b>QUICK SUMMARY OF HA PROBE OPERATIONS (FAILOVER AND FALLBACK) .....</b>	<b>28</b>
<b>TESTING HA FAILOVER AND TROUBLESHOOTING.....</b>	<b>29</b>
<b>HA BEST PRACTICES .....</b>	<b>32</b>
<b>DATA_ENGINE_ID SETTING ‘BEHAVIOR’ .....</b>	<b>33</b>
<b>NOTES ON UMP AVAILABILITY/FAILOVER .....</b>	<b>33</b>
<b>NOTES ON EMS .....</b>	<b>34</b>
<b>FAQS.....</b>	<b>35</b>

## Background

The UIM HA probe automates UIM failover to a Secondary (HA) hub, a.k.a. ‘failover’ or ‘standby’ hub. When the Primary hub goes down, the Secondary (HA) hub brings up the services the HA probe has defined in its HA.cfg file. The HA probe is installed on a Secondary hub. UIM core probes are not ‘HA-aware’ – they do not know the state of the Primary hub. If the configuration on the Secondary is the same as on the Primary (it may well not be for various reasons), the same alarms will be generated. How the Secondary nas deals with those alarms depends on how it's been configured. The HA probe doesn't use a ‘synchronization’ process – it uses a *heartbeat* to the Primary to determine if it is still available. If the heartbeat fails based on configured intervals, then it starts activating probes and queues on the Secondary.

Note that the HA probe does not ‘synchronize’ cfg files. It simply starts and stops queues and probes. Alarm synchronization is done by the nas internally, the HA probe does not have any part in that process.

Note also that any preprocessing (filters) needs to take place at the originating nas. Assuming that the Secondary hub is a ‘pure-play’ HA hub (passive), then it is NOT performing any preprocessing while it is in a passive state, as all robots that are directly reporting to one of the HA pairs are instead reporting to the Primary/active hub, up until failure of that hub. The Primary/active hub would have active preprocessing rules/filters based upon the incoming alarms from the robots and probes directly reporting up to it.

Upon failover, the HA probe resets and activates the NAS AO with all the same profiles, filters, triggers, and scripts as are on the Primary. The robots will then switch over to the Secondary and everything continues as it should from an alarm processing point of view. If the Secondary is actually an active remote hub node and is also there for load balancing the robots, then it can be a more complex scenario.

UMP failover is not fully covered in this document. UMP failover is currently not officially tested nor supported. You can search the DX Infrastructure Manager (UIM) communities for more information and use a LUA script or a probe available from Field Services to setup and test UMP failover.

The setup, installation/configuration, as well as testing of failover scenarios included in this document have been conducted in a Lab environment.

## High Availability Use Case Considerations

If the Primary hub has a planned or unplanned outage that may take more than a few hours to remedy, you may want to ensure that the failover hub has a full install—contains all of the same probes as the Primary for the sake of full Primary Core hub functionality. If you anticipate Primary hub shorter-term outages of 3 hours or less, you have the option to deploy just the essential probes for UIM HA to ensure the basic functions of the Primary hub continue.

This decision greatly depends on the business impact/criticality as well as the scale of your environment, e.g., impact on business operations, as well as whether or not there is a high volume of alarms generated in your current Production environment which require alerting and remediation.

Aside from the HA probe, you can use a **Microsoft Active/Passive cluster** to provide High Availability for UIM. Please refer to the following UIM Help doc link for more information:

<https://docops.ca.com/ca-unified-infrastructure-management/8-5-1/en/installing-ca-uim/install-uim-server/installing-in-an-active-passive-microsoft-cluster>

## UIM High Availability (HA)

The installation and configuration of a Secondary (HA) hub to provide failover in case the Primary hub becomes unavailable is a key step in the implementation of UIM.

This document will describe:

- How to setup a Secondary hub (a.k.a. 'standby' hub) for Primary Hub failover using the HA probe
- HA hub installation options
- HA Setup and Configuration
- How to perform Failover Testing
- How to Troubleshoot your HA setup
- Recommended Best Practices for HA

## Environment

- UIM v8.51
- Hub v7.93\_HF10
- Robot v7.93\_HF11
- HA v1.45 - check the release notes for important updates in HA v1.46 and 1.47.  
<http://support.nimsoft.com/unsecure/archive.aspx?id=142>
- nas v8.56
- OS: Windows 2012
- Database: Microsoft SQL Server 2012 SP1 Enterprise

**Note that HA failover was tested in UIM v9.02, v9.10, and v9.20 in our Support Labs. UMP failover (which is not officially supported), was also successfully tested in the lab. In all cases when testing with 9.x versions, the default probe versions for the 9.x installations were used.**

## HA setup instructions – summarized checklist

1. Setup Secondary (HA) Hub via manual installation, OR the UIM server installer
2. Deploy any/all probes that you need running on the Secondary hub during a failover if you are not using the UIM server installer, or if you need to install other probes that are not part of the standard UIM server install
3. Configure the Primary hub distsrv to Forward all probe packages AND Licenses to the Secondary
4. Configure the Secondary hub so that it contains the required queues for QOS and alarms (same as Primary)
5. Disable nas NiS Bridge on the Secondary (HA) hub
6. Configure nas alarm Forwarding & Replication on the Primary and Secondary hubs
7. Configure nas options for HA failover on the Secondary
8. Edit nas configuration files as needed
9. Copy nas scripts to Secondary
10. Configure HA probe/queue options
11. Test failover scenarios (Primary stopped/rebooted, etc.)
12. Troubleshoot failover if necessary
13. Save all HA-related configuration files

## UIM Secondary (HA) hub

The option to deploy a Secondary hub (a.k.a ‘standby’ hub) that can ‘take over’ for the Primary hub can be installed/setup in 2 ways.

### Option 1: Manual HA hub Setup

- Deploy the hub package and a list of other probe packages to the Secondary (HA) hub
- Note that the list of packages that you need on the HA hub may vary in future versions as probes and their dependent packages may change. Each subsequent UIM version may change the list of required/dependent packages, and some probes need several other packages.
- Follow steps 2 - 12 from the “HA setup instructions – checklist” section of this document.

### Option 2: HA hub installation (via UIM server installer)

Installing a Secondary (HA) hub using the UIM Server installation package, (setupcauimserver.exe).

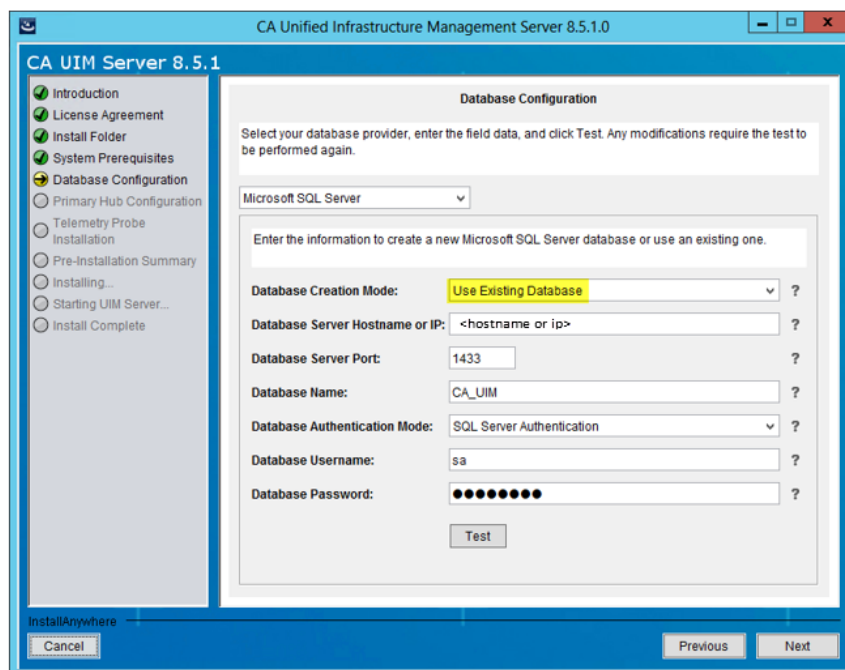
- Login to <http://support.nimsoft.com> and go to Downloads.
- Download the UIM server install package and UIM server packages

### Warning:

If you had any previously existing Secondary hub installs for High Availability, make sure you Deactivate the HA probe on that other hub and keep it deactivated, otherwise that hub will take over when the Primary hub is taken down and it will interfere with the UIM server installation option method.

The following instructions for Option 2 assume you are performing this installation on a clean system with no pre-existing UIM hub/robot installation.

- **IMPORTANT:** Make a copy of `/hub/security.cfg` on your Primary hub for safekeeping
- **Stop the Primary hub** (You can stop the Robot Watcher service to stop the hub)
- During the Secondary (HA) hub installation select the ***“Use existing database”*** option



- Follow the same installation instructions of a Primary hub
  - Specify the same domain that your current Primary hub and database belongs to, but use another (different) hub name.
  - Use the same userid/password combinations
  - When the installation is complete, install the Infrastructure Manager on the HA hub and then in IM select Security->Login and login to the newly installed hub.

If you choose Option 2 and install the Secondary (HA) hub using the UIM server installer, it will ensure all of the core/service probes and related queues are deployed and configured. But there is still configuration work to be completed.

Deactivate the data\_engine and all the dependent probes.

Probe	Port	PID	Version
<input type="radio"/> alarm_enrichment			8.42
<input type="radio"/> automated_deployment_engine			8.51
<input type="radio"/> baseline_engine			2.76
<input type="radio"/> cm_data_import			8.51
<input checked="" type="radio"/> controller	48000	1852	7.80
<input type="radio"/> data_engine			8.50
<input type="radio"/> discovery_agent			8.51
<input type="radio"/> discovery_server			8.51
<input checked="" type="radio"/> distsrv	48007	4000	5.40
<input type="radio"/> ems			9.01
<input type="radio"/> fault_correlation_engine			1.67
<input checked="" type="radio"/> hdb	48008	2300	7.80
<input checked="" type="radio"/> hub	48002	1596	7.80
<input type="radio"/> maintenance_mode			8.40
<input type="radio"/> mon_config_service			8.50
<input checked="" type="radio"/> mpse	48012	4780	1.72
<input type="radio"/> nas			8.42
<input type="radio"/> net_connect			3.31
<input type="radio"/> nis_server			8.51
<input checked="" type="radio"/> ppm	48025	4316	3.45
<input type="radio"/> prediction_engine			1.34
<input type="radio"/> qos_processor			8.50
<input type="radio"/> relationship_services			1.72
<input type="radio"/> rsp			5.20
<input type="radio"/> sla_engine			3.80
<input checked="" type="radio"/> spooler	48001		7.80
<input type="radio"/> telemetry			1.03
<input type="radio"/> topology_agent			1.72
<input type="radio"/> trellis			8.51
<input type="radio"/> udm_manager			8.51
<input type="radio"/> wasp			8.51

Then add them to the HA probe configuration. Note that with the UIM server install, the data\_engine connection is set and tested during the automatic install, but if manually installed, it must be reconfigured and tested manually to ensure the connection.

- Follow steps 3 - 12 from the “HA setup instructions – checklist” section of this document.

## Secondary (HA) Hub – Required and Optional Probes

The **essential** probes listed in blue font are highly recommended for HA setup. Those NOT in blue font are considered less essential/optional but please note that the examples and images contained within this document represent an HA deployment that includes full functionality for the Secondary hub.

- **HA**
  - used for failover
  - Recommendation: Activate it and keep it Activated after setup is complete
- **admin console**
  - Requires: adminconsoleapp, wasp and mps packages (mps, mpse)
  - Note that you can check Installed packages via the controller GUI.
  - As of UIM v8.42 or higher, follow this article IF needed but first check if you already have setup/access to the adminconsoleapp.
    - How to install a second instance of the web-based Admin Console application on a remote / secondary hub

<https://community.broadcom.com/enterprisesoftware/viewdocument/tech-tip-uim-how-to-install-a-se?CommunityKey=170eb4e5-a593-4af2-ad1d-f7655e31513b&tab=librarydocuments>

- **data\_engine**
  - used for inserting QoS into the database
  - Note that the data\_engine configuration raw and historical data retention settings should be set the same as the primary.
- **nas**
  - used for alarm display and processing, AO rules, scripts
  - Recommendation: keep it Activated
- **alarm\_enrichment**
  - used for enrichment of alarms. nas is dependent on AE
  - Recommendation: keep it Activated
- **distsrv**
  - used for access to local archive.
  - Recommendation: keep it Activated
- **emailgtw**
  - used for the ability to take actions on alarms, e.g., send alarm messages via email.
  - no need to create a queue for the emailgtw as a temp queue is created when it is deployed/installed
  - Recommendation: keep it Activated
- **wasp, mpse, ppm**
  - used for web admin console on the Secondary (HA) hub upon failover
  - Recommendation: Keep mpse and ppm activated but not wasp
- **discovery\_server**
  - Routes discovery data to the database. Collects status from discovery agents, collects information about the UIM Server infrastructure: hubs, robots, probes, packages, monitored systems or devices, monitored subsystems or items and monitored metrics, probes that publish discovery information and much more. Applies correlation rules to associate new device records, where appropriate, with any already-existing master device records
  - if deployed there is no need to create a queue for the discovery\_server as a temp queue is created when it is deployed/installed.
  - If you have any LUA scripts setup or manual 'excludes' in the discovery\_server directory, you need to move these manually to the same location on the Secondary hub



- **sla\_engine**
  - o for the ability to continue calculating SLAs if you have Service Level Agreements
- **ugs\_server**
  - (prior to 8.2)
  - **service\_host** and **admin\_console**, (or **wasp** depending on UIM version)
  - to provide access to the web Admin Console (adminconsoleapp)
  - runs the Admin Console web app
- **nis\_server**:
  - o As of UIM 8.31, you don't need nis\_server for UMP (USM) groups. UGS probe supersedes it. The nis\_server is not necessary on the secondary/HA hub. The UGS server does nis\_server's job as of UIM 8.31. But note that you do need it once again in UIM version 8.51 for UMP (USM) groups.
- **remote monitoring probes** (such as RSP)
  - o This ensures that the secondary hub can continue any remote monitoring that was being done by the primary hub.
- **qos\_processor** – dependent on data\_engine. The qos\_processor probe is not required. data\_engine can run without qos\_processor.
- **sla\_engine** – if you have SLAs
- **trellis** – application services container. Deployment of the alarm\_routing\_service is also required if you are fully using the ems probe.
- **ems** – requires trellis. The Trellis Application Container (trellis) probe contains services that are used by core UIM components such as data access services/das for
  - o Grouping in USM
  - o Health Index information
  - o The ems probe is currently not supported for HA failover. For more information see the section on ems at the end of this document.
- **nas\_api\_service**
  - o The nas\_api performs all database reads and writes for the alarm data in USM. The nas\_api service is automatically deployed as part of a UIM installation or upgrade.
- **alarm\_routing\_service**
  - o The alarm\_routing\_service is an *optional* service that is used with the ems probe. It routes legacy alarm messages to the ems probe for processing.
- **udm\_manager** – USM Groups
  - o UIM 8.1 or higher. udm\_manager is dependent upon the data\_engine probe to access UIM database connections. Several probes/components are dependent upon the UDM Manager probe for full functionality. Those probes/components

are: discovery\_server, ugs/trellis, and UMP. udm\_manager MUST be active for Discovery Server, USM, and UGS/Trellis to function

- **spectrumgtw** - requires ems and trellis. Note that the ems probe is not supported for failover in UIM 8.51 but is supported as of ems v10.20 or higher.

### Probes to keep Activated – checklist

**IMPORTANT:** Keep the following probes Activated/running on the Secondary Hub.

**Do NOT include them in the HA configuration enable/disable options.**

- **Robot** (controller, hdb, spooler)
- **distsrv** (archive packages, licenses) – distsrv is required for the data\_engine to start!!!
- **HA** (for failover)
- **hub** (take over for Primary)
- **nas** (alarm server)
- **alarm\_enrichment** (enrichment)
- **ppm, mpse** (so the web admin console remains available/accessible after failover to the Secondary hub. wasp will start up upon failover because it will use the local data\_engine.

### HA Hub Setup steps

Before shutdown, during configuration and testing, “Deactivate” all core/existing probes/other probes on the Secondary (HA) hub that are only needed on the Primary/*running* hub.

The screen shot below provides a picture of the state of the probes on the Secondary (HA) hub before any failover has occurred.

Probe	Port	PID	Version
ace		5380	8.42
alarm_enrichment		6588	8.56
baseline_engine		2576	2.76
controller	48000	3540	7.93
data_engine		3772	8.50
discovery_server		5444	8.52
distsrv	48007	5636	5.30
emailgtw		2856	2.84
ems		4640	9.01
HA	48010	6800	1.45
hdb	48008	1816	7.93
hub	48002	592	7.93
maintenance_mode		4036	8.40
mon_config_service		3952	8.52
mpse	48013	792	1.72
nas	48014	1208	8.56
net_connect			3.31
nis_server		3924	8.51
ntservices			3.27
ppm	48009	3600	3.40
prediction_engine		5336	1.34
processes			4.32
qos_processor		5748	8.50
sla_engine		4528	3.80
spectrumgtw		6392	8.64
spooler	48001		7.93
trellis		7148	9.00
udm_manager		5080	8.51
wasp			8.51

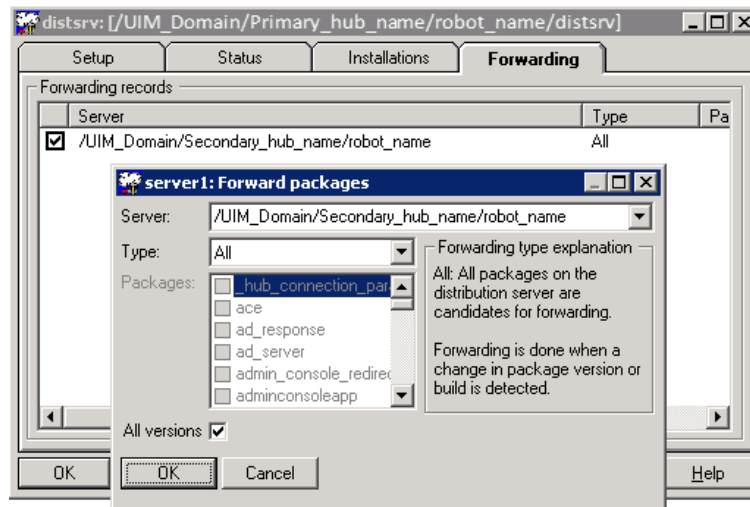
- Shutdown the Secondary (HA) hub (Stop the Robot)
- Start the Primary hub and login via Infrastructure Manager (or the adminconsoleapp)
- Once the Primary hub is fully active, Activate the Secondary (HA) hub (Start the Robot service)
  - In a *non-tunneled* Primary-Secondary (failover) hub configuration, if you have IM open and you don't see your Secondary (HA) hub appear, open the Primary hub configuration, select "Name services" and add a new Static hub entry for the Secondary hub, click OK, and select the IM login icon)
  - Note HA (v1.45 or higher) is also supported for two hubs across a tunnel. Please refer to the HA Release notes at: <http://support.nimsoft.com/unsecure/archive.aspx?id=142>

**Important Note:** At this point during startup of the Primary hub, UIM might prompt you to re-initialize the security on your Primary hub, if you left the Secondary (HA) hub running.

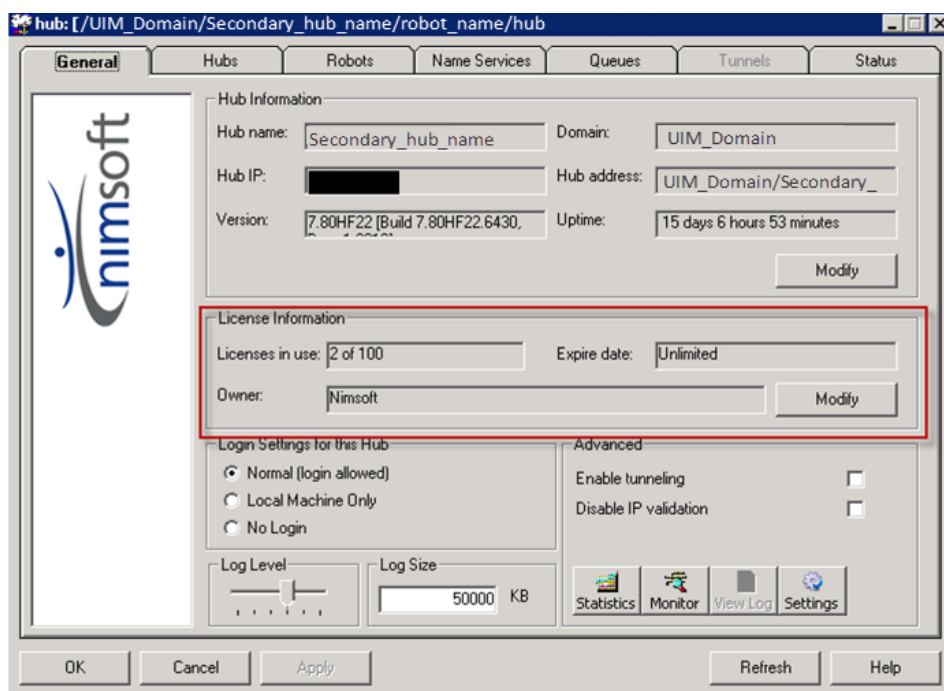
Do **NOT** re-initialize security!

## Configure Distribution Server and Licenses

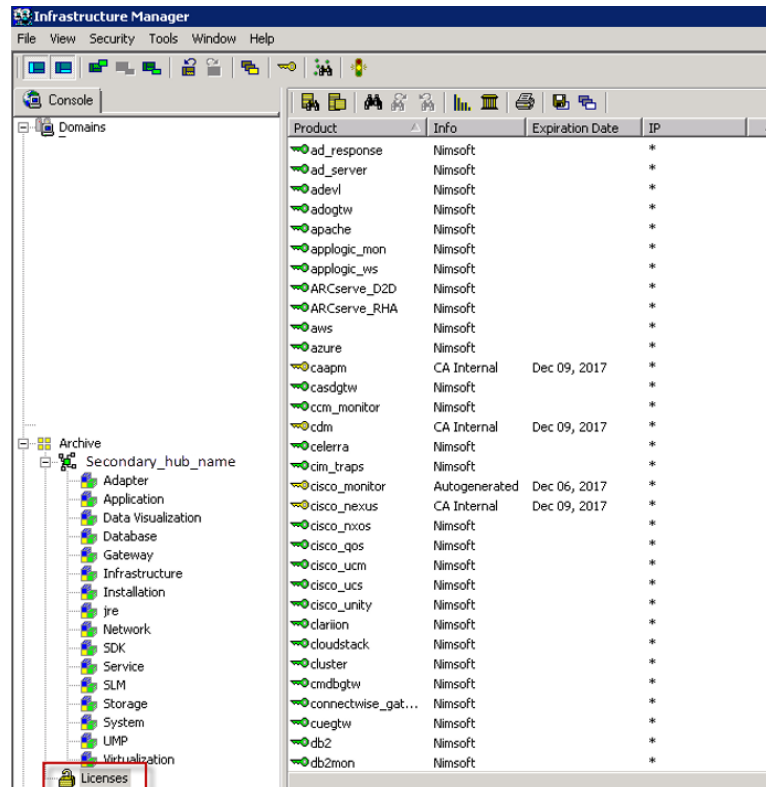
- Use the Infrastructure Manager (IM) on your Primary hub to create a distsrv forwarding rule for "All" packages and another rule for "All" Licenses on the **Primary** hub, **TO** your Secondary (HA) hub address, to ensure that your Primary and Secondary Archives stay in sync. If the NimBUS address of your HA hub does not display in the Server drop down window, you may add an entry for it via the Primary hub probe-> Name Services Tab (add the IP address). Then open the distsrv probe and try again.



- Check to make sure that you entered and confirmed the hub license as well as the probe licenses on both the Primary and Secondary hubs via the a) hub probe GUI 'General' Tab-> License Information and b) Archive->Licenses Icon window. Note that you can expedite license setup via Import of all of the required licenses for each hub.



- **Note:** Verify on your **Secondary** (HA) hub if you have the correct licenses. Otherwise, upon failover, you could experience problems where most of the important probes are not started because of license errors/expiration.



### Notes on Licensing when implementing HA in UIM v9.20 or higher:

Starting with UIM version 9.20 or higher, licenses are no longer required. Here is a screen shot of the Licenses portion of the hub GUI which shows what the Perpetual license would look like in the hub probe GUI for version 9.20 or later on the Primary and Secondary (HA) hubs.

License Information

Licenses in use: 
Expire date:

Owner:

For further information please refer to this link regarding UIM v9.20 and license dependencies:

<https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/9-0-2/release-notes/ca-uim-9-service-pack-1.html>

## Configure the Secondary (HA) hub so that it contains the required queues for QOS and alarms

- For any Secondary hub queues that don't already exist, re-create, or copy the related queues defined in the hub *postroute* section at ...\\Nimsoft\\hub\\hub.cfg on your Primary hub, **TO** your Secondary (HA) hub, but keep most of the queues *inactive*. Then Rt-click and restart the HA hub. Shown below are the Primary and Secondary hub Queues and Queue Status before any failover has occurred.

**Primary (Pre-failover)**

**Secondary (Pre-failover)**

hub: [/UIM\_Domain/Primary\_hub\_name/robot\_name/hub]

Name	Type	Subject/Queue	Address
<input checked="" type="checkbox"/> data_engine	attach	QOS_MESSAGE.QOS_DEFINITI...	
<input checked="" type="checkbox"/> nas	attach	alarm2	
<input checked="" type="checkbox"/> alarm_enrichment	attach	alarm	
<input checked="" type="checkbox"/> tot_rule_config	attach	TOT_RULE_CONFIG	
<input checked="" type="checkbox"/> baseline_engine.BASELINE_CONFIG	attach	BASELINE_CONFIG	
<input checked="" type="checkbox"/> prediction_engine.PREDICTION_CONFIG	attach	PREDICTION_CONFIG	
<input checked="" type="checkbox"/> probeDiscovery	attach	probe_discovery	
<input checked="" type="checkbox"/> udm_inventory	attach	udm_inventory	
<input checked="" type="checkbox"/> baseline_engine.QOS_MESSAGE	attach	QOS_MESSAGE	
<input type="checkbox"/> SYSLOG-QUEUE	attach	SYSLOG-IN	
<input type="checkbox"/> tickets	attach	alarm_assign,alarm_close,alarm...	
<input checked="" type="checkbox"/> emailgw	attach	EMAIL	
<input checked="" type="checkbox"/> qos_processor_qos_message	attach	QOS_MESSAGE	
<input checked="" type="checkbox"/> qos_processor_qos_baseline	attach	QOS_BASELINE	
<input checked="" type="checkbox"/> action_manager	attach	ems_action	
<input checked="" type="checkbox"/> legacy_alarm_manager	attach	legacy_alarm	
<input checked="" type="checkbox"/> alarm_manager	attach	enriched_events	
<input type="checkbox"/> ...	attach	TOT RULE CONFIG	

hub: [/UIM\_Domain/Secondary\_hub\_name/robot\_name/hub]

Name	Type	Subject/Queue	Address
<input type="checkbox"/> prediction_engine.PREDICTION_CONFIG	attach	PREDICTION_CONFIG	
<input type="checkbox"/> data_engine	attach	QOS_MESSAGE.QOS_DEFINITI...	
<input checked="" type="checkbox"/> nas	attach	alarm2	
<input checked="" type="checkbox"/> alarm_enrichment	attach	alarm1	
<input type="checkbox"/> tot_rule_config	attach	TOT_RULE_CONFIG	
<input type="checkbox"/> action_manager	attach	ems_action	
<input type="checkbox"/> legacy_alarm_manager	attach	legacy_alarm	
<input type="checkbox"/> alarm_manager	attach	enriched_events	
<input type="checkbox"/> ems	attach	TOT_RULE_CONFIG	
<input type="checkbox"/> event_manager	attach	event	
<input checked="" type="checkbox"/> udm_inventory	attach	udm_inventory	
<input type="checkbox"/> alarm-routing-service	attach	alarm	
<input type="checkbox"/> baseline_engine.QOS_MESSAGE	attach	QOS_MESSAGE	
<input type="checkbox"/> baseline_engine.BASELINE_CONFIG	attach	BASELINE_CONFIG	
<input checked="" type="checkbox"/> SECONDARY_HUB_probe_discovery	attach	probe_discovery	
<input checked="" type="checkbox"/> SECONDARY_HUB_QOS	attach	QOS_MESSAGE.QOS_DEFINITI...	
<input type="checkbox"/> probeDiscovery	attach	probe_discovery	

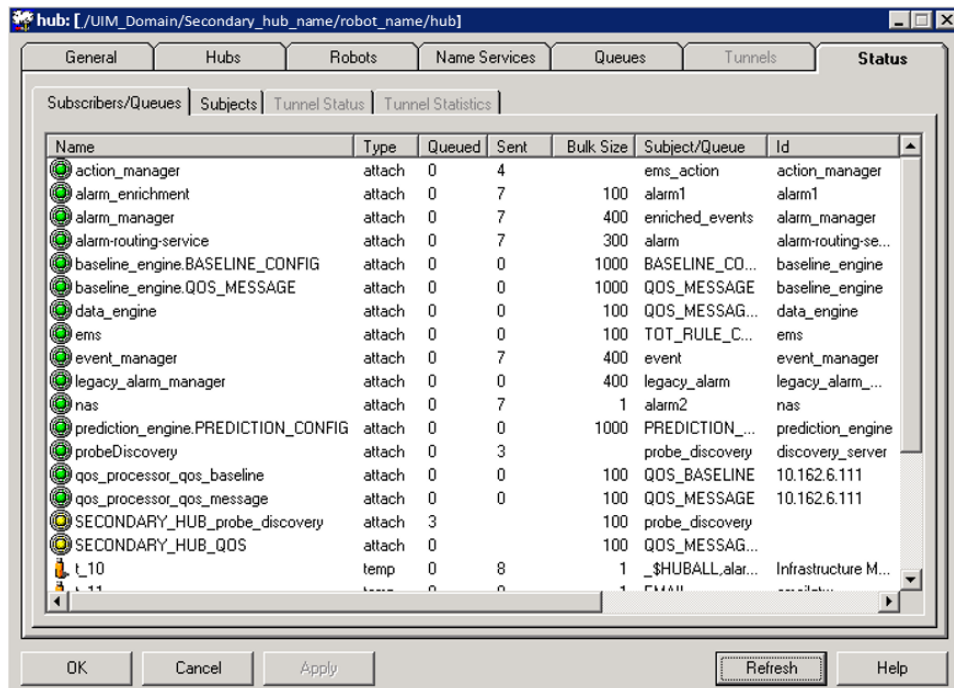
hub: [/UIM\_Domain/Primary\_hub\_name/robot\_name/hub]

Name	Type	Queued	Sent	Bulk Size	Subject/Queue	Id
<input checked="" type="checkbox"/> action_manager	attach	0	27	100	ems_action	action_u...
<input checked="" type="checkbox"/> alarm_enrichment	attach	0	60	100	alarm	alarm
<input checked="" type="checkbox"/> alarm_manager	attach	0	19	400	enriched_events	alarm_r...
<input checked="" type="checkbox"/> baseline_engine.BASELINE_CONFIG	attach	0	0	1000	BASELINE_CO...	baseline
<input checked="" type="checkbox"/> baseline_engine.QOS_MESSAGE	attach	0	91094	1000	QOS_MESSAGE	baseline
<input checked="" type="checkbox"/> data_engine	attach	0	690	100	QOS_MESSAGE	data_er...
<input checked="" type="checkbox"/> DISCOVERY_FROM_SECONDARY_NO_FAILOVER	get	0	6	100	SECONDARY_...	
<input checked="" type="checkbox"/> emailgw	attach	0	0	100	EMAIL	emailgw...
<input checked="" type="checkbox"/> ems	attach	0	0	100	TOT_RULE_C...	ems
<input checked="" type="checkbox"/> event_manager	attach	0	19	400	event	event_r...
<input checked="" type="checkbox"/> legacy_alarm_manager	attach	0	0	400	legacy_alarm	legacy_...
<input checked="" type="checkbox"/> nas	attach	0	60	1	alarm2	nas
<input checked="" type="checkbox"/> prediction_engine.PREDICTION_CONFIG	attach	0	0	1000	PREDICTION_...	predicti...
<input checked="" type="checkbox"/> probeDiscovery	attach	0	15	100	probe_discovery	discove...
<input checked="" type="checkbox"/> QOS_FROM_SECONDARY_NO_FAILOVER	get	0	470	100	SECONDARY_...	
<input checked="" type="checkbox"/> qos_processor_qos_baseline	attach	0	0	100	QOS_BASELINE	10.130...
<input checked="" type="checkbox"/> qos_processor_qos_message	attach	0	437	100	QOS_MESSAGE	10.130...
<input checked="" type="checkbox"/> L_D	temp	0	24	1	alarm_new,alar...	Alarm Li...
<input type="checkbox"/> ...	temp	0	0	1	...	...

hub: [/UIM\_Domain/Secondary\_hub\_name/robot\_name/hub]

Name	Type	Queued	Sent	Bulk Size	Subject/Queue	Id	Establ
<input checked="" type="checkbox"/> alarm_enrichment	attach	0	48	100	alarm1	alarm1	11/14
<input checked="" type="checkbox"/> nas	attach	0	0	1	alarm2	nas	11/15
<input checked="" type="checkbox"/> SECONDARY_HUB_probe_discovery	attach	0	6	100	probe_discovery	hub(magka04...	11/15
<input checked="" type="checkbox"/> SECONDARY_HUB_QOS	attach	0	477	100	QOS_MESSAG...	hub(magka04...	11/15
<input checked="" type="checkbox"/> L_180	temp	0	11	1	alarm_new,alar...	Alarm List [admi...	11/15
<input checked="" type="checkbox"/> L_181	temp	0	11	1	alarm_new,alar...	Alarm List [admi...	11/15
<input checked="" type="checkbox"/> L_182	temp	0	3	1	_SHUBALL	discovery_server	11/15
<input checked="" type="checkbox"/> L_91	temp	0	447	1	_SHUBALL.alar...	Infrastructure M...	11/14
<input checked="" type="checkbox"/> udm_inventory	attach	0	0	100	udm_inventory		

## Secondary (HA) Hub queues post failover



Name	Type	Queued	Sent	Bulk Size	Subject/Queue	Id
action_manager	attach	0	4		ems_action	action_manager
alarm_enrichment	attach	0	7	100	alarm1	alarm1
alarm_manager	attach	0	7	400	enriched_events	alarm_manager
alarm-routing-service	attach	0	7	300	alarm	alarm-routing-se...
baseline_engine.BASELINE_CONFIG	attach	0	0	1000	BASELINE_CO...	baseline_engine
baseline_engine.QOS_MESSAGE	attach	0	0	1000	QOS_MESSAGE	baseline_engine
data_engine	attach	0	0	100	QOS_MESSAGE...	data_engine
ems	attach	0	0	100	TOT_RULE_C...	ems
event_manager	attach	0	7	400	event	event_manager
legacy_alarm_manager	attach	0	0	400	legacy_alarm	legacy_alarm_...
nas	attach	0	7	1	alarm2	nas
prediction_engine.PREDICTION_CONFIG	attach	0	0	1000	PREDICTION_...	prediction_engine
probeDiscovery	attach	0	3		probe_discovery	discovery_server
qos_processor_qos_baseline	attach	0	0	100	QOS_BASELINE	10.162.6.111
qos_processor_qos_message	attach	0	0	100	QOS_MESSAGE	10.162.6.111
SECONDARY_HUB_probe_discovery	attach	3		100	probe_discovery	
SECONDARY_HUB_QOS	attach	0		100	QOS_MESSAG...	
t_10	temp	0	8	1	_SHUBALL,alar...	Infrastructure M...

- **Primary Hub GET Queues**
  - Define QOS 'GET' queues on the Primary hub to 'get' the data\_engine and probe\_discovery ATTACH queue messages from the Secondary hub (so that you get the QoS messages from any/all monitoring probes that are deployed on your Secondary hub as well as any QOS generated by Robots that belong to the Secondary hub).
- **Tunnels**
  - If you have tunnels defined on the Primary hub you will need to define them on your Secondary hub as well so tunnel operation will continue when the Secondary takes over.
  - The GET queues for any tunnels on the Secondary can remain INACTIVE. You can Activate them via the HA probe configuration/setup.
- **LDAP**
  - Note that if you enabled the LDAP configuration on your Primary hub you can install/configure the LDAP interface also on your Secondary hub but make sure the Secondary can connect to the LDAP server.
- **Additional Probes**

Deploy any needed *additional* probes to your Secondary hub, like emailgtw, helpdesk / gateway probes, etc.



Copy any customized [<probe>.cfg](#) files from the Primary hub since any additional customization you did on the Primary hub that you want to run on your Secondary hub during failover, needs to be identical, in place and customized on your HA hub as well.

- **Consider all of the probes that run on your Primary hub and decide if their operation is required upon failover.** For example, if RSP is performing remote monitoring from the Primary hub, you may want to enable it on the HA hub so monitoring is not interrupted. Similarly, you may also want to deploy other probes such as `discovery_server` to ensure discovery data continues to flow to the database tables.

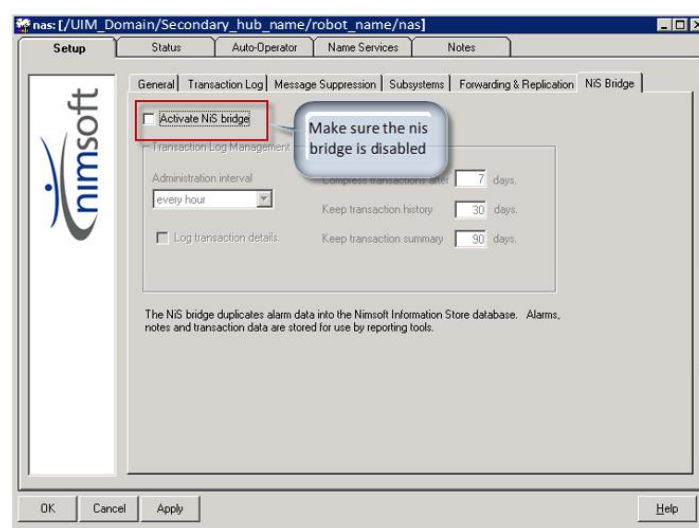
### Gateway probes

Lastly, on the Secondary (HA) hub, check the configuration and test connectivity for any gateway probes, e.g., `sdgtw`, `spectrumgtw`, etc., you have deployed and running on the Primary Hub.

If you implement HA according to this document you will have all the basic functions running during failover, but it is difficult to document all of the additional probes/queues/rules you might need to add after the basic HA setup. Therefore, try to take as much of your Primary Hub's configuration into account as possible when making your decisions and also refer to the list of probes contained in this document in the section titled: "Secondary (HA) Hub – Required and Optional Probes."

## Disable nas NiS Bridge

On the Secondary (HA) hub, nas probe configuration, Disable the nas NiS Bridge. In the nas Raw Configuration (`nis_bridge = no`). Note that only 1 NAS can update the UIM backend database tables with alarms via the NiS Bridge, so do NOT enable the nas NiS bridge on the HA hub, as this will result in database constraint violation errors in the NAS log. These errors do not cause any serious database issues, but it does result in a steady stream of error messages until the primary NAS successfully imports data into the backend NIS database.

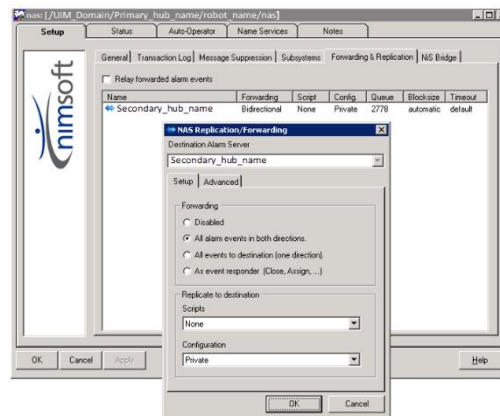




## Configure NAS alarm 'Forwarding & Replication' on Primary & Secondary (HA) hub

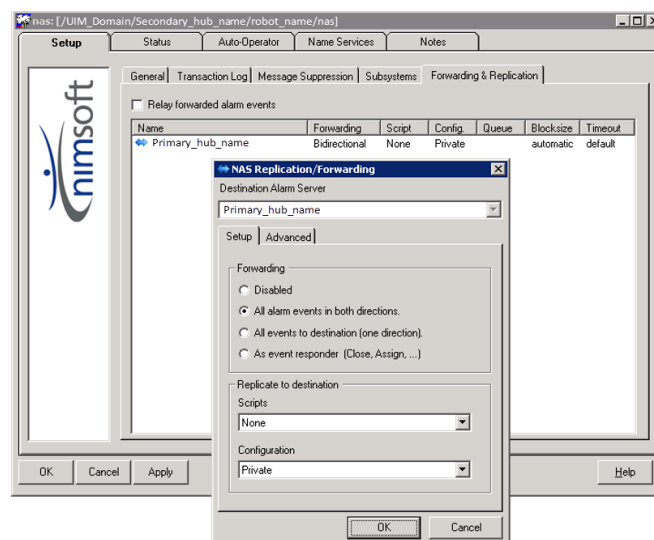
On the Primary hub, nas probe GUI configuration Tab: "Forwarding & Replication" - RT-click in the window to create a NAS Forwarding & Replication rule TO the Secondary hub.

- Set the Destination Alarm Server (Secondary Hub NimBUS address)
- Forwarding: Select All alarm events in both directions
- Select "None" for Scripts
- Select "Private" for Configuration
- Click Ok and then Click Apply



### Enable Forwarding & Replication rule on the Secondary (HA) hub as well.

- Set the Destination Alarm Server (Primary Hub NimBUS address)
- Forwarding: Select All alarm events in both directions
- Select "None" for Scripts
- Select "Private" for Configuration
- Click Ok and then Click Apply



**Destination Alarm Server**

Select the Destination alarm server from this list.

This is the alarm server with which you want to exchange alarms and/or scripts.

**Forwarding:**

Select the forwarding properties for the selected nas:

**All alarm events in both directions**

All alarm events will be sent to and received from the NAS selected as the Destination alarm server.

**Scripts**

Select if you want the scripts available on the NAS 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.

**Configuration**

Select if you want the configuration settings (profiles) available on the NAS to also be available for the destination alarm server defined.

*None* means not available for the destination alarm server 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

If you want to use this configuration file on the destination server, you must edit the file and then paste it manually to [\Nimsoft\probes\service\nas\nas.cfg](#).

### Tips on nas replication and forwarding configuration

If your Primary and Secondary (HA) hub are on the same network, but the Secondary (HA) hub is not displaying in the Infrastructure Manager (IM) navigation pane on the left side in IM, you most likely have to add Name Services entries for both hubs.

1. Add a Name Services entry via the hub GUI Name Services Tab-window on the Primary hub and enter the IP address of the Secondary (HA) hub and click ok.
2. Open the hub GUI on the Secondary (HA) hub and enter the IP address of the Primary Hub.
3. After refreshing your IM view via F5, the Secondary (HA) hub should now be displayed in the IM navigation window on the left side of the IM client window.

If you receive a popup error during the process of trying to add a new entry for nas replication and forwarding, such as:

**"Unable to locate any alarm servers in this domain that supports the new forwarding and replication services (version >= 3.0)."**

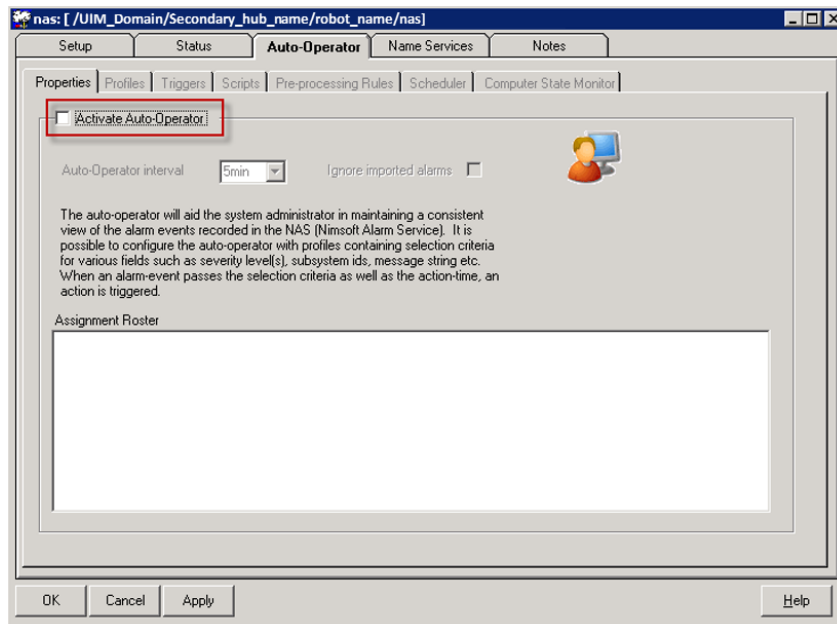
1. Restart the nas probe on the Primary and the Secondary
2. Select Tools->Options and configure the IM session to point to the Primary
3. Chose Security->Login and log back in to IM
4. Open the nas probe on either hub and you should now be able to successfully add a new nas replication and forwarding entry without any popup error and continue with the HA configuration

### Relay forwarded alarm events (optional)

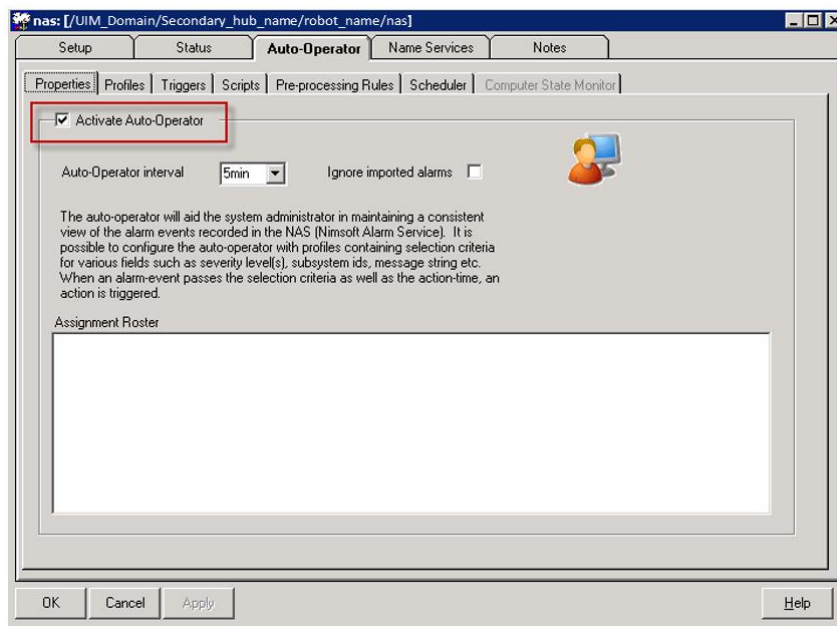
Checking the "Relay forwarded alarm events" option, alarms received from a remote nas will be forwarded.

### Configure Nas Auto-Operator on the Secondary (HA) hub

During nas setup on the Secondary (HA) hub, uncheck this option to disable the Secondary nas Auto-Operator so you don't cause duplicate alarm processing, e.g., two emails sent for a single alarm. The screen shot below depicts the state of the nas Auto-Operator configuration with AO disabled, after fallback to the Primary has occurred.



The screen shot below depicts the state of the nas Auto-Operator configuration with AO enabled, **after failover to the Secondary (HA) hub**.



Note that any replication alarms from the HA nas should be accepted as a normal occurrence and handled, e.g., an admin may acknowledge the alarm or close/exclude it via an AO rule on the Primary hub. Example alarm message:

*“Replication services failed for alarm server 'Primary\_hub\_name', reattempting.”*

ID	Message	Count	Host Name	Source	Time Received
HX29001758-04257	Replication services failed for alarm server 'Primary_hub_name', reattempting.		Primary_hub_name	10. [REDACTED]	11/15/17 19:41:19

## Required NAS Configuration file edits

If you are configuring the nas on the Secondary (HA) hub via the nas GUI on the Secondary, you can skip the following section regarding manual file edits.

The primary nas.cfg file will be replicated intact (as is) TO the Secondary (HA) hub server. As indicated above, it is copied to a location from which it needs to be moved in order for it to be read, and in effect on the failover hub's nas. Therefore, before it can be moved to the Secondary (HA) hub and put into effect, there are two edits that need to be completed first.

### 1. The nas Auto-Operator **MUST** be disabled

- Find and change the following "active = yes" to "**active = no**":

Before editing:

```
<auto_operator>
<setup>
  interval = 5min
  active = yes
  ignore_import = no
</setup>
```

After editing:

```
<auto_operator>
<setup>
  interval = 5min
  active = no
  ignore_import = no
</setup>
```

- The replication section may need to be changed if it contains the settings appropriate to the Primary nas, but its worth checking to be sure.

- a. Example before editing

```
<replication>
  relay = no
  <Secondary_hub_name>
    name = Secondary_hub_name
    alarms = 1
    scripts = 2
    config = 1
  </Secondary_hub_name>
</replication>
```

- b. Example after editing (for nas forwarding and replication TO the Primary)

```
<replication>
  <Primary_hub_name>
    name = Primary_hub_name
    alarms = 1
  </Primary Hub>
</replication>
```

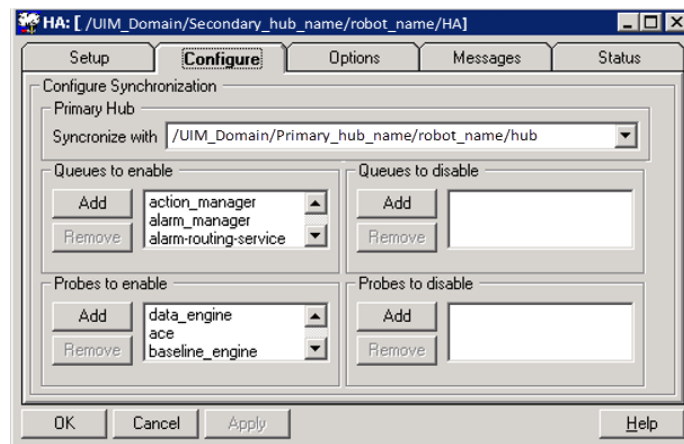
Once set, confirm the two settings via nas Raw Configure.

## Scripts folder

**The nas Scripts folder (entire contents) should be manually copied from the Primary hub nas to the Secondary (HA) hub nas, essentially replacing the Scripts folder and contents there.** If the hubs are Linux/Unix, the permissions that were assigned on the Primary hub will NOT be carried over to the Secondary (HA) hub nas. Observation shows that the permissions on the script files on the Primary hub are 755 but once replicated, the permissions change to 666 on the Secondary hub. This may or may not have any significant consequences for the nas probes ability to execute the scripts as it is the embedded LUA process that executes the scripts. This premise should be tested and if the permissions cause a problem, they should be changed. For Windows hubs, this will have no effect.

## HA probe configuration

- Deploy the HA probe onto the **Secondary** (HA) hub. Note that when it is deployed, it will remain deactivated and **grey**). Do **NOT** Activate it yet. Double-click to open the HA probe.
- Select the correct Primary hub NimBUS address in the 'Synchronize with' dropdown window.



## Queues to enable

You can change the order in which queues and/or probes are enabled or disabled upon failover. The following section presents some examples of queues from a Test environment. In a real Production environment, in the HA GUI you will see displayed, all possible GET queues you created on your Primary hub that GET all QOS and alarms from ATTACH queues defined on your remote hubs (tunneled and not tunneled). Here is an example of the `queue_up` section of the HA.cfg:

```
<queue_up>
queue_0 = action_manager
queue_1 = alarm_manager
queue_2 = alarm-routing-service
queue_3 = baseline_engine.BASELINE_CONFIG
queue_4 = baseline_engine.QOS_MESSAGE
queue_5 = data_engine
queue_6 = ems
queue_7 = event_manager
queue_8 = legacy_alarm_manager
queue_9 = prediction_engine.PREDICTION_CONFIG
queue_10 = probeDiscovery
queue_11 = qos_processor_qos_baseline
queue_12 = qos_processor_qos_message
queue_13 = tot_rule_config
queue_14 = udm_inventory
</queue_up>
```

## Probes to enable

Probes **MUST** be in the correct order based on probe startup order / prerequisite probe dependencies.

### IMPORTANT:

If you don't respect the correct order you will have some probes that will not start, for example because a prerequisite probe that must start before it, is not fully activated yet. If the

data\_engine doesn't start, e.g., because the distsrv was not left Activated/running, then many other probes that are dependent upon the data\_engine will not start and they will appear **red**.

Here is an example of the **probes\_up** section of the HA.cfg. Notice that the data\_engine is listed first. Before you test failover, check the HA.cfg file to ensure the probes/queues are in the correct order.

```
<probes_up>
  probe_0 = data_engine
  probe_1 = ace
  probe_2 = baseline_engine
  probe_3 = prediction_engine
  probe_4 = emailgtw
  probe_5 = discovery_server
  probe_6 = udm_manager
  probe_7 = ems
  probe_8 = trellis
  probe_9 = maintenance_mode
  probe_10 = mon_config_service
  probe_11 = qos_processor
  probe_12 = sla_engine
  probe_13 = spectrumgtw
  probe_14 = nis_server
  probe_15 = wasp
</probes_up>
```

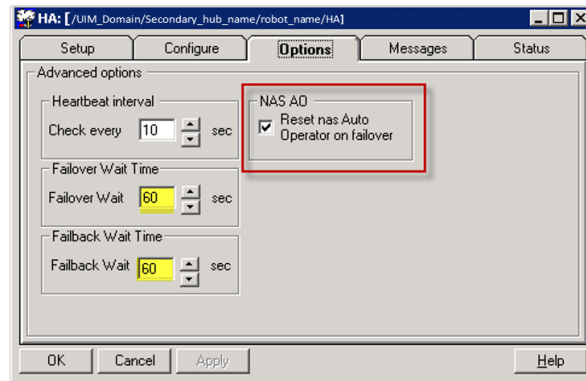
## Key probe startup/operational dependencies for HA

Here are some of the key probe dependencies you need to be keep in mind when deciding upon the probe startup sequence.

- distsrv MUST start before data\_engine (keep the distsrv up/running and NOT in the HA.cfg)
- data\_engine MUST start before service\_host/wasp to avoid logging invalid errors
- alarm\_enrichment MUST start before nas
- baseline\_engine MUST start before prediction\_engine, but note that normally it is not advisable to have baseline\_engine and the prediction\_engine activated and operating on the Primary hub due to resource utilization/overhead. Normally they run on remote hubs. Hence, they can be deactivated and removed from the HA configuration.
- Prior to 8.5.1, admin\_console is a web app run by service\_host, so it does not appear in the list of probes to enable, and neither does mps or uimserver\_home



## HA Options Tab Settings



### Failover Wait time

How long the HA probe waits for a response from the Primary hub before it instructs the Secondary hub to take over. The default wait time is 30 seconds.

### Fallback Wait time

How long the HA probe waits after communication with the Primary hub has been re-established before it begins fallback, thereby allowing time for all probes, tunnels, and queues configured on the Primary hub to be ready. The default wait time is 30 seconds.

### Reset nas Auto Operator on failover

Select this option to enable Auto-Operator on the nas probe running on secondary hub on failover. If selected, the Auto-operator setting in the nas configuration is modified and the nas probe is restarted. If the 'Reset nas Auto Operator on failover' option is enabled in the HA probe it should ACTIVATE the Auto-Operator (AO) Tab on failover and Deactivate it on fallback.

The purpose of the Secondary (HA) hub as it relates to the Nimsoft Alarm Server (nas) is to temporarily take over for the Primary hub when it goes down so that your Auto-Operator pre-processing rules and profiles continue to be applied to your alarms upon failover. When failover occurs, the Secondary (HA) nas will start and continue to store alarms in its own local database files. Then when the Primary hub is back up and its nas is running again, the nas on the Secondary (HA) hub will TRANSFER any alarms from its local database tables that have come in while the Primary hub was down, via the configured nas Forwarding and Replication rule/queue configured on the Secondary (HA) hub. In this manner, the nas on the Primary hub will update its local database tables and also update the NAS tables in the UIM database through the NiS bridge when the Primary is back up.

## HA Testing

### Test and Adjust HA/nas settings if necessary

Keep in mind that it's a manual task to copy / create / update your existing nas Auto-Operator (AO) profiles on the Secondary hub.

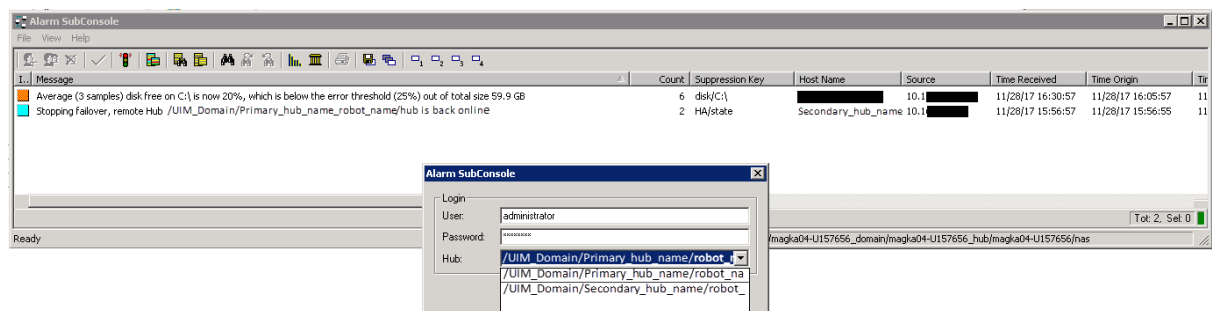
---

*At this point you can try a first failover test by stopping the Primary hub (stop the Robot Watcher service) and verify if all probes and all queues on the Secondary (HA) hub have activated.*

---

Note: During testing and switching back and forth from the Primary to the Secondary and back, you can start up and follow the alarm flow via the **AlarmSubConsole.exe** client (located in C:\Program Files (x86)\Nimsoft\bin. The alarm subconsole client doesn't need UMP and can serve later as a backup alarm console. You can switch which hub it connects to using File->Login.

### Alarm subconsole view



### Activate the HA Probe

After disabling probes on the Secondary (HA) hub except the robot (controller, hdb and spooler), distsrv, hub, nas, alarm\_enrichment, mpse, ppm, and wasp probes), go ahead and Activate the HA probe. Then check the HA.log to make sure it is checking the status of the Primary via the default 10s heartbeat, for example:

```
Nov 9 15:04:06:780 HA: INFO: checking connection to
'/UIM_Domain/Primary_hub_name/robot_name/hub' (10.130.xxx.xxx)
Nov 9 15:04:06:780 HA: SREQUEST: _status ->10.130.xxx.xxx/48002
Nov 9 15:04:06:780 HA: RREPLY: status=OK(0) <-10.130.xxx.xxx/48002 h=37 d=291
```

### Stop the Primary Hub (Robot)

When you purposely STOP the Robot on the Primary hub you can see from the HA.log that the connection is lost, for example:

```
Nov 9 15:09:26:942 HA: WARN: Failed to contact primary hub
'/UIM_Domain/Primary_hub_name/robot_name/hub', retry_count: 0, return_code: 2,
error_txt: communication error.
Nov 9 15:09:28:065 HA: sockConnect - connect to 10.130.xxx.xxx 48002 failed
10061
```



update their status and show as deactivated/disabled (turn **grey**) in the Infrastructure Manager (IM).

The HA.log will contain a message regarding fallback:

```
HA: INFO: primary hub is back online, sleeping for fallback wait_time: 60
```

And then finally, upon fallback to the Primary, the last alarm displays:

```
Stopping failover, remote Hub '/UIM_Domain/Primary_hub_name/robot_name/hub'
is back online
```

The aforementioned HA alarms do not clear automatically.

On fallback, it may take 1-2 mins or so for the probes to deactivate/turn **grey** again on the HA hub. Please refer to the screen shot below for an example of how it would appear, depending on what probes/queues are disabled after falling back to the Primary.

Note that the probes on the Secondary (HA) hub should not be Activated (**green**) OR be displayed in an error state (**red**). If you see this occur, then there is most likely something wrong with the configuration or order (probe sequence) of bringing the probes/queues up or down

upon fallback to the Primary hub. Most commonly, red status may be due to the probe startup order or probe *dependencies*, e.g., probes that are dependent upon the data\_engine or some other probe that needs to be fully started first. Probes that are purposely kept Activated/running will be green and that is expected but if a probe is still Activated/Running and green, when it should not be, then double-check the HA probe configuration.

Probe	Port	PID	Version
<input type="radio"/> ace			8.42
<input checked="" type="radio"/> alarm_enrichment	48016	244	8.56
<input type="radio"/> baseline_engine			2.76
<input checked="" type="radio"/> controller	48000	1692	7.80HF21
<input type="radio"/> data_engine			8.50
<input type="radio"/> discovery_server			8.52
<input checked="" type="radio"/> distsrv	48012	5500	5.30
<input type="radio"/> emailgtw			2.84
<input type="radio"/> ems			9.01
<input checked="" type="radio"/> HA	48007	1812	1.45
<input checked="" type="radio"/> hdb	48008	3364	7.80HF21
<input checked="" type="radio"/> hub	48002	2012	7.80HF22
<input type="radio"/> maintenance_mode			8.40
<input type="radio"/> mon_config_service			8.52
<input checked="" type="radio"/> mpse	48011	5936	1.72
<input checked="" type="radio"/> nas	48019	5892	8.56
<input type="radio"/> net_connect			3.31
<input type="radio"/> ntservices			3.27
<input checked="" type="radio"/> ppm	48009	280	3.40
<input type="radio"/> prediction_engine			1.34
<input type="radio"/> processes			4.32
<input type="radio"/> qos_processor			8.50
<input type="radio"/> sla_engine			3.80
<input type="radio"/> spectrumgtw			8.64
<input checked="" type="radio"/> spooler	48001		7.80HF21
<input type="radio"/> trellis			9.00
<input type="radio"/> udm_manager			8.51
<input checked="" type="radio"/> wasp	48010	168	8.51

When the Primary hub becomes available again, the Secondary will detect that it is back online again and it will generate an alarm notification:

```
Stopping failover, remote Hub /UIM_Domain/Primary_hub_name/robot_name/hub is back online
```

If you see alarm messages of this type show up in the alarm subconsole from the Secondary Hub:

```
Failed to get status of queue qos_processor_qos_baseline, please check it  
Failed to get status of queue qos_processor_qos_message, please check it
```

These messages normally indicate that these queues are either missing or misconfigured. Otherwise, if the queues referenced in the alarm are green and processing messages, the alarms can be ignored, or acknowledged and were probably caused by some timing issue. In testing, I only saw this happen with the qos\_processor probe queues. The messages, if generated should be cleared when the queues are activated and processing messages.

## Quick Summary of HA probe operations (failover and fallback)

Under normal HA operation, the HA probe will perform the following functions:

- Check the Primary hub status every n seconds
- Failover hub operations to the Secondary (HA) hub if the Primary does not respond
  - Enable/Disable probes and queues (configurable)
- Continue checking the Primary, e.g., every 10 seconds
- When the Primary hub is back up/online, fallback to the Primary hub
- Disable probes and queues on the Secondary (HA) hub when quiescent

If you have other hubs that normally send QoS/Alarms to the Primary, you will need to make the appropriate changes here. The remote hubs will have some ATTACH queues that require corresponding GET queues. You would have a GET queue on the primary to get the data from the remote side, so you will need to do the same, create a GET queue on the HA hub.

For some helpful UIM HA diagrams that illustrate data flow during normal operations versus failover, please refer to:

<https://docops.ca.com/ca-unified-infrastructure-management/8-0/en/managing/manage-hubs/set-up-high-availability-for-the-primary-hub>

## Testing HA Failover and Troubleshooting

### Test Environment:

- UIM v8.51
- Hub v7.93\_HF10
- Robot v7.93\_HF11
- HA v1.45
- nas v8.56
- Database: Microsoft SQL Server 2012 SP1 Enterprise

During HA testing, you can manually stop the Robot to take down the Primary hub. Normally it takes approximately 30-60 seconds to shutdown the Hub (Robot).

Another test you can perform is to reboot the Primary Hub. When the Primary Hub failover occurs, an **Informational** alarm is generated and seen in the console:

*Initiating failover from remote Hub /UIM\_Domain/Secondary\_hub\_name/robot\_name/hub*

Then when the Primary Hub boots up, check the HA log to make sure the HA hub took over, and the fallback occurred after the Primary was back up again.

### Primary Hub Reboot Scenario

The following HA.log entries are taken from a test scenario where the Primary was rebooted.

#### ...Reboot of Primary, and its not up yet...

```
Nov 16 09:51:55:233 HA: WARN: Failed to contact primary hub  
'/UIM_Domain/Primary_hub_name/robot_name/hub': communication error. Issuing  
state change.
```

#### ...Primary hub finishes booting up...

```
Nov 16 09:52:25:586 HA: INFO: UpdateCache - updated remote hub information:  
10.130.xxx.xxx  
Nov 16 09:52:25:587 HA: INFO: checking connection to  
'/UIM_Domain/Primary_hub_name/robot_name/hub' (10.130.xxx.xxx)  
Nov 16 09:52:25:590 HA: SREQUEST: _status ->10.130.xxx.xxx/48002  
Nov 16 09:52:25:593 HA: RREPLY: status=OK(0) <-10.130.xxx.xxx/48002 h=37 d=294  
Nov 16 09:52:25:593 HA: sockClose:0000000000B7B200:10.162.x.xxx/64029  
Nov 16 09:52:25:593 HA: SREQUEST: _close ->10.130.xxx.xxx/48002  
Nov 16 09:52:25:593 HA: INFO: Connection to  
'/UIM_Domain/Primary_hub_name/robot_name/hub' restored. Issuing state change.  
....  
Nov 16 09:52:25:593 HA: INFO: primary hub is back online, sleeping for fallback  
wait_time: 60  
Nov 16 09:53:25:595 HA: INFO: Fallback wait time expired. Continuing with  
fallback actions.
```

```
Nov 16 09:53:25:595 HA: INFO: expanded 'Restored contact with remote Hub  
$remote_hub' to 'Restored contact with remote Hub  
/UIM_Domain/Primary_hub_name/robot_name/hub'
```

### **...HA then deactivates the configured probes and queues on the Secondary (HA) hub...**

```
Nov 16 09:53:25:598 HA: INFO: state == 'HA_DEACTIVATE'  
etc...  
etc...
```

Note that once the Primary is taken down you will need to login via IM TO the Secondary (HA) hub. If you have the web admin console setup on the Secondary, you can also access it via a browser at: [http://<uim\\_server>/adminconsoleapp](http://<uim_server>/adminconsoleapp)

Note that queues from any remote hubs (QOS/data) may take ~2 minutes to turn green after a failover.

### **HA functionality - details**

HA determines whether it needs to failover or not by performing a “ping” to the hub. It uses the *nametoip* call to find the IP for the hub it is a failover for. So, one thing to check is to run a *nametoip* callback from the controller and/or hub of the failover/secondary hub to see what it thinks the primary is. If it is wrong this could mean you have an outdated/corrupt hubs.sds file. A bad hubs.sds file could cause the HA probe to failover because *nametoip* returned an incorrect IP.

### **Connectivity**

Also, check your network connectivity. Run a ping from one hub to another for a few hours and see if you have any periods of dropped packets. Run a tracert. Check name resolution via nslookup. Note that ‘unexpected’ failover to the Secondary hub could be caused by network connectivity/latency/environmental issues.

### **Licenses**

After you configure the HA probe on the Secondary hub, if you bring down the Primary to test the failover, you may see a message that 'Failover is being initiated...' but after that you also see that the data\_engine probe does not start and turns red. Alarms are generated and you see in the alarm console, data\_engine probe alarm messages like:

```
"Data_engine failed - Probe 'data_engine' (command = data_engine.exe) returns  
no-restart code (42) "
```

and

```
"No valid SLM-QOS license was found"
```

If the Secondary/HA hub doesn't have the correct licenses for the data\_engine it will not start and you will see errors in the data\_engine log such as:

```
Nov 8 14:51:34:875 [1588] de: GetLicense - no license found for 'SLM-QOS'
```

```
Nov 8 14:51:34:875 [1588] de: GetLicense - no license found for 'SLM-SLA'
Nov 8 14:51:34:875 [1588] de: GetLicense - no license found for 'SLM-GUI'
Nov 8 14:51:34:875 [1588] de: License SLM-QOS:
Nov 8 14:51:34:875 [1588] de: License SLM-SLA:
Nov 8 14:51:34:875 [1588] de: License SLM-GUI:
Nov 8 14:51:34:890 [1588] de: SLMFactory::NewSLM - Requesting MS SQL Server
Nov 8 14:51:35:015 [1588] de: You need a license for SLM-QOS to run this
probe
```

To resolve this issue, double-check to make sure you have configured the distsrv on the Primary hub to forward All probes as well as All Licenses to the Secondary (HA) hub as part of the configuration.

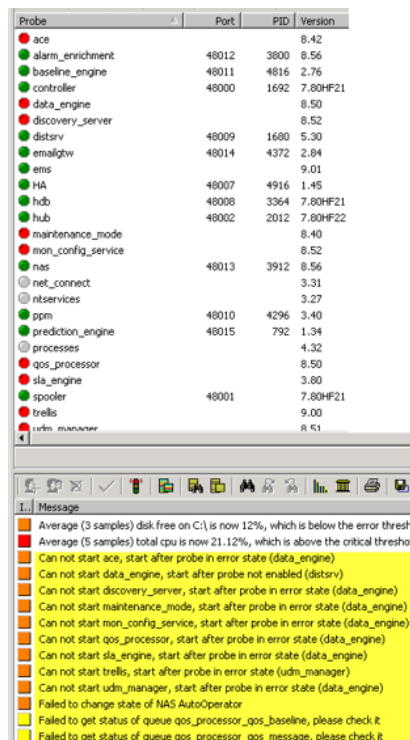
## Enrichment

Note on enrichment - if alarm\_enrichment messages are queuing up and not sending any alarms as per the hub status GUI, check the log and if the log is stuck at connecting to the database and you see no updates to the log, test the connection to the database using the correct host, e.g., shortname versus longname to make sure you have that specified correctly in the nas alarm\_enrichment configuration (cmdbs section).

## Probes turn red on the Secondary

If you dont get the order of probes right and/or a dependency is ignored, you will see alarms like this in the console on failover to the Secondary (HA) hub:

*"Can not start <probe>, start after probe in error state (<prerequisite probe>)," or ... "start after probe not enabled (<probe name>)."*





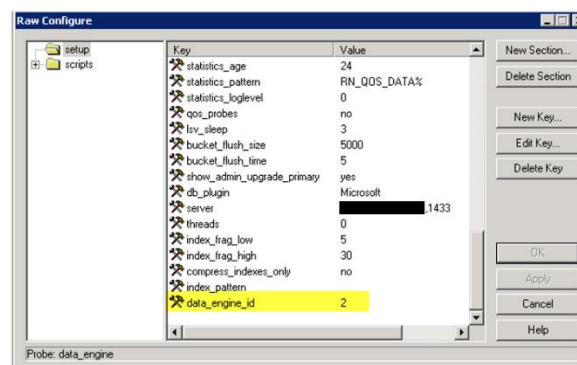
Once the settings are correct and the order of the probes/queues is rectified, and all dependencies are satisfied as well, then those alarms will no longer occur.

## HA Best Practices

- ☐ Since the probes running on the HA hub have their own configuration files and monitoring profiles, you can be selective about whether you want to enable full monitoring upon HA failover. You may choose to enable a subset of the probes, monitor fewer systems, or use less frequent polling during failover.
- ☐ Install Infrastructure Manager (IM) on the Secondary (HA) hub if you normally access the IM on the Primary hub. This is not necessary if you have Infrastructure Manager on a computer other than the primary hub, and you manage your components from there.
- ☐ Confirm that you can run the admin console application from the Secondary hub as well.
- ☐ Check to make sure that the version of each probe on the Primary matches the Secondary (HA) node
- ☐ NIS bridge can only be active on one nas at a time
- ☐ HA solution should generally be used when the primary is down for short time periods, e.g., no more than a few hours, for an alternative failover solution we recommend Microsoft Windows Cluster.
- ☐ Backup and safeguard all HA-setup related configuration files from the Secondary hub, HA.cfg, nas.cfg, hub.cfg, robot.cfg, data\_engine.cfg, etc.
- ☐ In general, we recommend that no 'monitoring' probes are present on either the Primary or Secondary hubs, just the *core* infrastructure probes.

### data\_engine (Primary versus Secondary mode)

After the data\_engine probe package is installed/deployed to the Secondary (HA) hub machine, then configured to connect to the database server, the **data\_engine\_id** parameter is added to the data\_engine.cfg and set to 2 automatically. This setting determines the data\_engine's role as Primary or Secondary. 1 is for Primary and 2 is for the Secondary (HA) hub (see below). Note that data\_engine *maintenance* is always disabled on the Secondary.



## Data origin - Secondary (HA) hub

- After you finish the Secondary (HA) hub install (whether manually or via installer) you may elect to change the origin of the Secondary (HA) hub via the hub settings, to the same hub origin as the Primary. Otherwise, the QOS it generates will contain a different origin than the Primary hub. But note that you may not want to leave it that way if post failover the Secondary hub goes back to its role as a remote hub with its own origin and robots attached to it.
- This also applies to any 'HA-paired' hub, e.g., collector (tunnel server) hubs. HA-paired hubs are hubs paired up for failover for any set of Secondary hubs. For example, you have two tunnel servers and one of them is an HA backup node for the first one. The backup node must use the same origin as the tunnel server hub that it is backing up.
- In the majority of cases an "HA" hub doesn't have its own set of robots/probes. The Secondary (HA) hub is normally dedicated for failover. Therefore, in that case, it makes the most sense to make the origins match so that the data will be "seamless," but in some rare cases that might not be the case.

## data\_engine\_id setting 'behavior'

- The **data\_engine\_id** setting value is stored in the **tbn\_de\_controller** table. The manner of install (manual setup versus UIM server installer) should not matter when it comes to how the data\_engine\_id in the database is altered. Neither manual nor automatic install should set the **data\_engine\_id** on a Secondary (HA) hub to 1. It should always be set to 2 and the The data\_engine on the Primary hub should remain set to 1.
- The **data\_engine\_id** does **NOT** change on failover and/or failback. The data\_engine id on the Primary hub is set to 1, Secondary (HA) hub remains set to 2.

```
select * from tbn_de_controller
```

Id	SPId	Address	State	TimeRegister	TimeReregister
1	57	/UIM_Domain/Primary_hub_name/robot_name/data_engine	primary	2017-01-10 17:48:26.380	2017-11-20 16:30:02.617
2	51	/UIM_Domain/Secondary_hub_name/robot_name/data_engine	secondary	2017-11-08 14:47:46.823	2017-11-17 12:55:11.310

## Notes on UMP availability/failover

DX Infrastructure Manager (UIM), does not currently test or support UMP High Availability/failover. If the primary hub fails, you need to manually point wasp to the HA hub as there is no automated UMP failover.

Note also that during failover mode, when the Secondary is active, no alarm updates will make their way to UMP. You can view the alarms in the alarm sub-console.

That stated, for field-developed probes/scripts that can be leveraged for UMP failover, please search the Broadcom DX Infrastructure Manager (UIM) community at:

<https://community.broadcom.com/enterprisesoftware/communities/communityhomeblogs?CommunityKey=170eb4e5-a593-4af2-ad1d-f7655e31513b>

**IMPORTANT:** Note that in UIM v9.x versions when implementing UMP failover, you must ensure you copy the cryptkey from the Primary to any UMP node(s).

Copy the original certificate.pem over from the Primary to the Secondary (HA) hub directly. (no copy/paste). Then ensure that the absolute path to its location on the file system is referenced in the robot.cfg. For example:

C:\Program Files (x86)\Nimsoft\security\certificate.pem

Here is a reference to one important KB article regarding HA configuration in UIM 9.02/9.20:

UMP and CABI wasp probes won't start when moved to HA hub and reconfigured

[https://ca-broadcomcsdm.wolkenservicedesk.com/wolken/esd/knowledgebase\\_search?articleId=138976](https://ca-broadcomcsdm.wolkenservicedesk.com/wolken/esd/knowledgebase_search?articleId=138976)

## Notes on EMS

In UIM v8.5.1 (and ems probe v9.0x), the ems probe does **not** currently support failover.

EMS uses an embedded database for operational purposes with storage under the db folder in the ems probe directory. This folder includes open (active) alarms, closed alarms, and various bits of state such as rule states and schedules. The db sync that you see in the log at loglevel 5 is from an optional process that exports open alarms only to a set of tables in the nis (backend UIM) database, e.g., ems\_alarm, etc. Closed alarms and state are not exported. Further, the export of active alarms is one-way—there is no method to recreate the active alarms in the embedded database from the tables in the nis db. So, while the probe can be restarted and the log seems to indicate all is well post-failover, the reality is that there is currently no way to failover and restore the optional state. Customers could implement something using the existing capabilities in the EMS but this would be a custom services type of activity.

Lastly, to validate ems behavior, you must first have alarms flowing into the EMS. i.e., you must set up alarm routing, define routes, etc., to get alarms to actually flow into the EMS. Then you can pull the plug on the primary EMS and failover to a Secondary. You should find that all the alarms managed by the EMS are no longer visible in the UMP/USM alarm view.

---

*Note that as of UIM 9.x, when running ems version 10.20 or higher, ems is HA aware/compliant for failover.*

---

Also, a new parameter “isprimary” has been added to the ems probe. By default, when the ems probe is running on the Primary hub, this is set as True. When the failover happens and ems is running on the secondary hub, the parameter ‘isprimary = false’.

## FAQs

### **1. In an HA environment, what other configuration do you normally recommend (if any) related to how to configure the environment, e.g., robots/other hubs to work with the Primary and Secondary (HA) node on failover and failback?**

Robots that are reporting to the Primary hub should have the Secondary (HA) hub configured as the secondary hub. Therefore, the configuration should be changed on robots/hubs to work with the HA setup, e.g., this is configured via the robot/controller under "Setup -> Nimsoft -> Secondary HUB" section.

ATTACH queues are already configured on the remote hubs. GET queues must be configured on both the Primary AND the HA hub. The GET queues on the Primary hub are active and the GET queues on the HA hub are deactivated. The HA probe is configured to activate them on failover. Tunnels between the Primary and remote hubs AND between the HA hub and remote hubs are configured and active at all times.

If you're using Named Services (Static hubs), the remote hubs are configured on both the Primary and HA hub Named Services and the both the Primary and HA hub are configured in the remote hub Named Services.

### **2. As it relates to the nas/ems, on a failover event, will the HA node/secondary be able to keep alarms in sync out of the box?**

You have to configure bi-directional forwarding and replication on the nas.

### **3. Any risks/disadvantages in HA operation?**

There are a few disadvantages for instance, UMP failover and CABI (bundled) operation upon failover are not 'officially' supported/tested.

### **4. Are there other failover alternatives?**

Ideally, we recommend using MSCS for the most *transparent* approach to failover, but it introduces an added cost. For more detailed information please refer to:

#### **Installing in an Active/Passive Microsoft Cluster**

<https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/it-operations-management/unified-infrastructure-management/9-0-2/installing/install-uim-server/installing-in-an-active-passive-microsoft-cluster.html>