

IMS

DX Infrastructure Observability

Global Support Team

**High Availability (HA) Guide
DX UIM 23.4 CU3**

Updated: February 25, 2025

Author: Steve Danseglio

Table of Contents

BACKGROUND	2
HIGH AVAILABILITY USE CASE CONSIDERATIONS	2
UIM HIGH AVAILABILITY (HA)	3
ENVIRONMENT	3
HA SETUP INSTRUCTIONS – SUMMARIZED CHECKLIST	4
UIM SECONDARY (HA) HUB	4
OPTION 1: MANUAL HA HUB SETUP.....	4
OPTION 2: HA HUB INSTALLATION (VIA UIM SERVER INSTALLER).....	5
SECONDARY (HA) HUB – REQUIRED AND OPTIONAL PROBES	7
PROBES TO KEEP ACTIVATED – CHECKLIST.....	10
CONFIGURE DISTRIBUTION SERVER	11
CONFIGURE THE SECONDARY (HA) HUB SO THAT IT CONTAINS THE REQUIRED QUEUES FOR QOS AND ALARMS	14
DISABLE NAS NIS BRIDGE.....	17
CONFIGURE NAS ALARM ‘FORWARDING & REPLICATION’ ON PRIMARY & SECONDARY (HA) HUB	17
<i>Tips on nas replication and forwarding configuration</i>	<i>19</i>
CONFIGURE NAS AUTO-OPERATOR ON THE SECONDARY (HA) HUB	20
REQUIRED NAS CONFIGURATION FILE EDITS	21
SCRIPTS FOLDER	23
HA PROBE CONFIGURATION	23
QUEUES TO ENABLE	24
PROBES TO ENABLE.....	24
KEY PROBE STARTUP/OPERATIONAL DEPENDENCIES FOR HA	25
HA TESTING	26
SECONDARY (HA) HUB POST-FAILOVER	29
SECONDARY (HA) HUB PROBE STATUS AFTER FALLBACK	30
QUICK SUMMARY OF HA PROBE OPERATIONS (FAILOVER AND FALLBACK)	31
TESTING HA FAILOVER AND TROUBLESHOOTING.....	32
HA BEST PRACTICES	34
DATA_ENGINE_ID SETTING ‘BEHAVIOR’	38
NOTES ON OC AVAILABILITY/FAILOVER	38
NOTES ON DEPLOYING SPECTRUMGTW.....	39
FAQS.....	42

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 sends a *heartbeat* to the Primary to determine if it is still available. If the heartbeat test fails based on the defined, configured intervals, then it starts activating probes and queues on the Secondary (HA) Hub.

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, so 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 should have active preprocessing rules/filters based upon the incoming alarms from the robots and probes directly reporting to it.

Upon failover, the HA probe resets and activates the NAS Auto Operator (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 could be a more complex scenario.

Operator Console (OC) failover is not fully covered in this document. OC 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, which is available via the UIM community to setup and test OC failover.

The setup, installation, configuration, as well as testing of failover scenarios included in this document have been conducted in the Broadcom 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: [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 23.4.3
- Hub 23.4.3
- Robot 23.4.3
- HA 20.40
 - Release notes: <http://support.nimsoft.com/unsecure/archive.aspx?id=142>
 - HA probe is only supported on Windows_x64 and Linux_x64 OS platforms
- nas 23.4.3.2
- Infrastructure Manager (IM) 23.4.3
 - Always upgrade IM to the same version you've installed/upgraded to, e.g., 23.4.3.
- OS: Windows 2016 Datacenter
- Database: Microsoft SQL Server 2016 Enterprise 2016 (SP3-OD) (KB5006943) - 13.0.6404.1 (X64)
- data_engine schema version: 20.45(0)
- Network: Primary and Secondart (HA) hub failover and failback works on preferably the same network, or the same subnet, or a dfferent network via use of a tunnel.

HA setup instructions – summarized checklist

1. Setup Secondary (HA) Hub via manual installation, or preferably run the uimserver installer after stopping the Primary hub-robot.
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/custom probes, etc., 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 and 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 auto operator (AO) rules/scripts to the Secondary (HA) hub
10. Configure HA probe/queue 'options'
11. Test failover scenarios (Primary stopped/rebooted, etc.)
12. Troubleshoot failover if necessary
 - a. Main logs to examine include HA.log, nas.log, hub.log, controller.log
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)

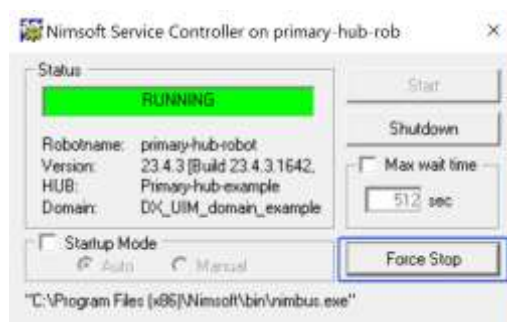
Installing a Secondary (HA) hub using the UIM Server installation package, (setupCAUIMServer)

- Login to <http://support.nimsoft.com> and go to Downloads.
- Download the UIM server installer file (setupCAUIMServer) and uimserverpackages.zip

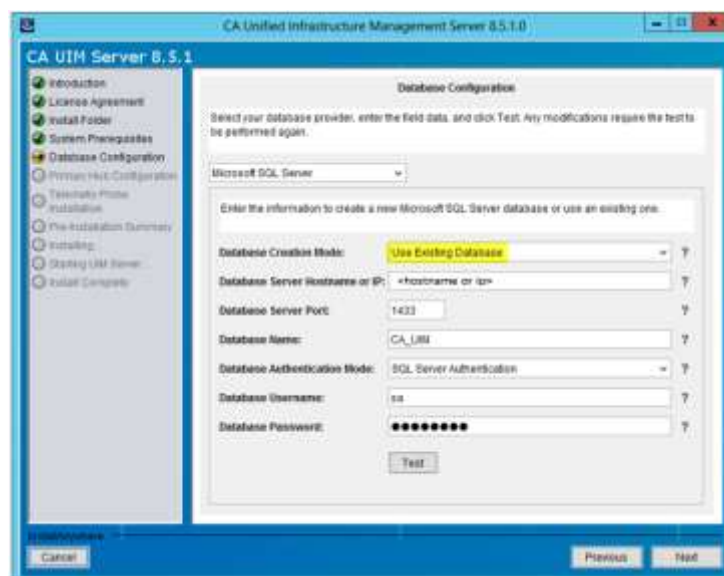
WARNING!

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 (Use Force Stop)**
You can stop the Nimsoft Robot Watcher Service to stop the hub-robot
- Use the Nimsoft Service controller utility and click 'Force Stop' and leave the Nimsoft service controller dialog window open on the Primary so you can access it to stop and start the Primary hub quickly and easily when testing failover.



During the Secondary (HA) hub installation select the “Use existing database” option



- Follow essentially the same installation instructions as a Primary hub
 - Specify the same domain that your current Primary hub and database belongs to, but use another (different) hub name for this HA Hub and robot.
 - Use the same userid/password combinations
 - When the installation is complete, install the appropriate version of the Infrastructure Manager on the HA hub from the Installers link on the /uimhome page which displays after the install process completes
 - Then in IM select Security->Login and login to the newly installed hub.

If you choose Option 2 as above, and install the Secondary (HA) hub using the UIM server installer, it will ensure all of the core/service probes, and their related queues are deployed and configured. This is the best practice and the preferred approach but there is still some configuration work to be completed.

On Windows, note that after you download the UIM server installer, if the installer hangs on mounting, Rt-click and choose Properties, then choose "Unblock All." You simply need to manually change the file properties to allow execution.

Deactivate the data_engine and all the dependent probes on the HA hub. An example is provided below.

Probe	Class	Version
alarm_enrichment	Probe/Port	23.4.3.2
automated_deployment_engine	Probe/Port	23.4.3
baseline_engine	Probe	23.4.3
cdm	Probe	7.20
cm_data_import	Probe	23.4.3
configuration_reader_service	Probe/Port	23.4.3
controller	Probe/Port	23.4.3
data_engine	Probe	23.4.3
discovery_agent	Probe	23.4.3
discovery_server	Probe	23.4.3
distsrv	Probe/Port	23.4.3
emailgtw	Probe	2.91
ems	Probe	23.4.3
HA	Probe/Port	20.40
hdb	Probe/Port	23.4.3
hub	Probe/Port	23.4.3
maintenance_mode	Probe	23.4.3
mon_config_service	Probe	23.4.3
mpse	Probe/Port	23.4.3
nas	Probe/Port	23.4.3.2
net_connect	Probe	3.44
nis_server	Probe	23.4.3
ntservices	Probe	3.60
ppm	Probe/Port	23.4.3
prediction_engine	Probe	23.4.3
qos_processor	Probe	23.4.3
rsp	Probe	5.59
sla_engine	Probe	23.4.3
spectrumgtw	Probe	20.41
spooler	Probe/Port	23.4.3
telemetry	Probe	23.4.0
usage_metering	Probe	9.4.2
wasp	Probe	23.4.3
webgtw	Probe	23.4.3

As part of the process, we will add the probes under “Probes to enable” in 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 to the backend UIM database is successful.

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: Keep it deactivated until the HA hub is installed.
- **Admin console**
 - Requires: adminconsoleapp, wasp and mps packages (mps, mpse)
 - Follow this article IF needed but first check if you already have setup/access to the adminconsoleapp and the 23.4.3 version packages are already present.
 - You can check ‘Installed packages’ via the controller GUI->Status Tab.
 - IMPORTANT NOTE: The hub(s) on which admin console is installed must be able to directly access the backend UIM database.
 - For this reason, the admin console cannot be deployed to "remote" Secondary hubs, e.g., those connected via a tunnel to the core environment.) It can only be deployed to hubs that are within the same internal network/LAN/subnet so that the hub/wasp can communicate directly with the database server.

How to install a 2nd instance of the Admin Console application on the Secondary (HA) hub

After the Secondary (HA) hub is installed, stop the Primary hub-robot so it fails over to the Secondary (HA) Hub. This is required since the wasp probe on the HA machine needs to be able to connect to the database.

1. From the local archive, deploy the adminconsoleapp, wasp and mps packages (mps, mpse).
2. Confirm you can access the admin console using your local web browser on the HA hub, e.g., http://<HA_hub_hostname_or_IP>/adminconsoleapp



Status	Hub	Address	License	IP	Version	Port
✓	ha-hub-example	/DX_UIM_domain/example/ha-hub-example/ha-hub-01	true	11	23.4.3 (Build 23.4.3.1367, Dec 31, 2024)	48002
✗	Primary hub-example	/DX_UIM_domain/example/primary-hub-example/primary	true	11	23.4.3 (Build 23.4.3.1367, Dec 31, 2024)	48002
✓	sample-detachhub1	/DX_UIM_domain/example/sample-detachhub1/sample-d	true	11	23.4.2 (Build 23.4.2.1343, Aug 4, 2024)	48003
✓	vxhub01-example	/DX_UIM_domain/example/vxhub01-example/vxhub01	true	11	23.4.3 (Build 23.4.3.1367, Dec 31, 2024)	48002

AC access/performance check:

- Using the Admin Console app, test accessing a few probes such as cdm, processes. Then if present, test opening up the snmpcollector probe to see how long it takes to open up the configuration.
- **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 startup is dependent on alarm_enrichment.
 - 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.
 - Download the emailgtw from <http://support.nimsoft.com> to the Secondary (HA) hub, then Import it into the local archive, then deploy it via drag and drop to the secondary (HA) hub., There is no need to manually create a queue for the emailgtw as a temp queue is created when it is deployed/installed
- **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_agent**

- **automated_deployment_engine**
 - provides powerful functions to deploy robots and probes using XML distribution, and probe and package distribution in Admin Console.
- **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.
 - The discovery_server should always be activated on the Primary hub to receive discovery messages and process the robot_nis_cache messages.
 - If you have any LUA scripts setup or manual 'excludes' in the discovery_server directory, you must move these manually to the same location on the Secondary hub
- **sla_engine**
 - for the ability to continue calculating SLAs if you have Service Level Agreements and/or need to run queries from the OC SLM
- **nis_server:**
 - persists and populates groups created in the Operator Console (OC) user interface. Groups/Automatic grouping.
- **remote monitoring probes** (optional, such as RSP, net_connect, etc.)
 - This ensures that the Secondary (HA) hub can continue any remote monitoring that was already being performed by the primary hub.
- **qos_processor**
 - Dependent on data_engine, performs post-processing of QoS data by performing the following functions:
 - QoS baseline data management
 - Origin modification
- **ems**
 - event and alarm management service
- **alarm_routing_service**
 - 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. The alarm_routing_service and queue can be deactivated/deleted if its not being used.
- **spectrumgtw**
 - Alarm and inventory integration with NetOps Spectrum

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.

- [alarm_enrichment](#) (enrichment)
- [automated_deployment_engine](#)
- [configuration_reader_service](#)
- [discovery_agent](#) (keep it up and running on the HA hub)
- [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)
- [mpse](#)
- [nas](#) (alarm server)
- [ppm](#) (so the web admin console remains available/accessible after failover to the Secondary hub. wasp will still 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

Probe	Port	PID	Version
alarm_enrichment	48009	10200	23.4.3.2
automated_deployment_engine	48013	5884	23.4.3
baseline_engine			23.4.3
cdm			7.20
cm_data_import			23.4.3
configuration_reader_service			23.4.3
controller	48000	6956	23.4.3
data_engine			23.4.3
discovery_agent	48015	6976	23.4.3
discovery_server			23.4.3
distsrv	48007	9008	23.4.3
emailgtw			2.91
ems			23.4.3
HA	48012	3368	20.40
hdb	48008	6356	23.4.3
hub	48002	9184	23.4.3
maintenance_mode			23.4.3
mon_config_service			23.4.3
mpse	48020	8736	23.4.3
nas	48022	6548	23.4.3.2
net_connect			3.44
nis_server			23.4.3
ppm	48016	8016	23.4.3
prediction_engine			23.4.3
qos_processor			23.4.3
rsp			5.59
sia_engine			23.4.3
spectrumgtw			20.41
spooler	48001		23.4.3
telemetry			23.4.0
usage_metering			9.4.2
wasp			23.4.3
webgtw			23.4.3

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

- Stop 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, all probes are expected to be up and running, will display green icons, and have a port and a PID.
- Activate the Secondary (HA) hub (just start the Robot service using the service controller).
 - 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" tab and add a new Static hub entry using the IP for the Secondary hub, click OK, and select the IM login icon)

Note: HA probe as of (v1.45 or higher is also supported for two hubs across a tunnel. Please refer to the HA Release notes for more information at:

<http://support.nimsoft.com/unsecure/archive.aspx?id=142>

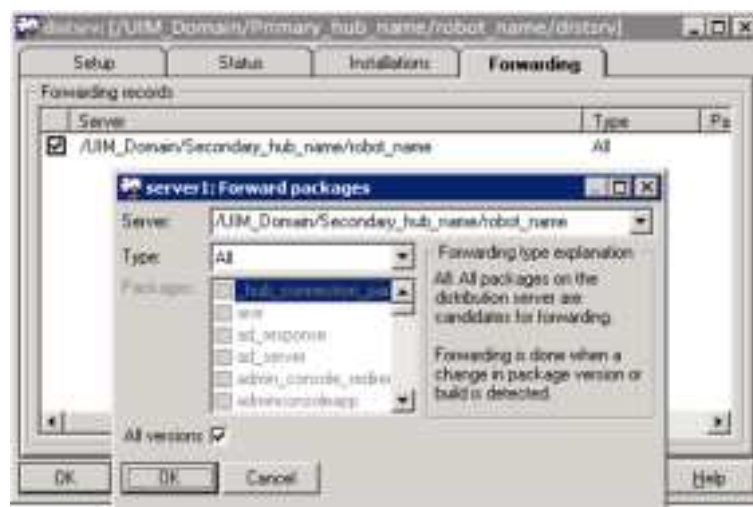
Important Note: At this point during startup of the Primary hub, the IM may prompt you to re-initialize the security on your Primary hub, if you left the Secondary (HA) hub running.

IMPORTANT!!!-> Do NOT re-initialize security!

- Follow steps 3 - 12 from the "**HA setup instructions – summarized checklist**" section of this document.

Configure Distribution Server

- Use IM on your Primary 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 the Primary and Secondary Archives stay in sync. If the NimBUS address of your HA hub does not display in the Server dropdown window, 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.





Note 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.



Secondary (HA) Hub probes pre-failover

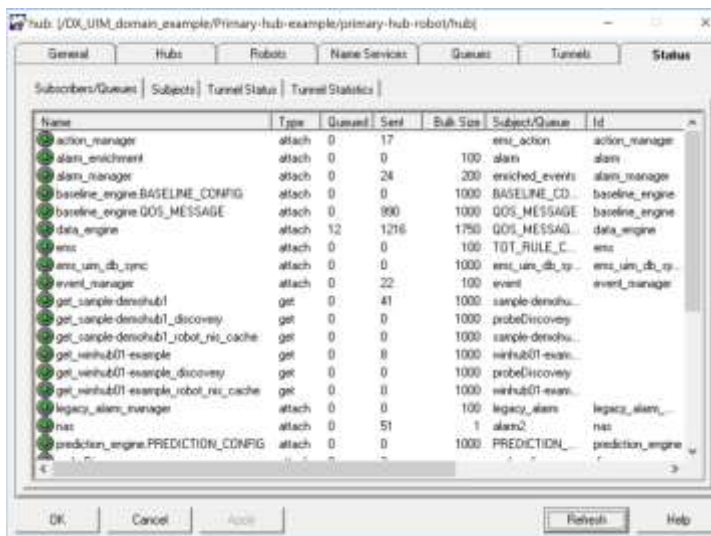
Probe	Port	PID	Version
alarm_enrichment	48013	7416	23.4.3.2
automated_deployment_engine	48010	5936	23.4.3
baseline_engine			23.4.3
cdm			7.20
cm_data_import			23.4.3
configuration_reader_service			23.4.3
controller	48000	5604	23.4.3
data_engine			23.4.3
discovery_agent	48015	7260	23.4.3
discovery_server			23.4.3
distsrv	48007	4880	23.4.3
emailgtw			2.91
ems			23.4.3
HA	48009	4772	20.40
hdb	48008	536	23.4.3
hub	48002	5728	23.4.3
maintenance_mode			23.4.3
mon_config_service			23.4.3
mpse	48011	7956	23.4.3
nas	48014	7656	23.4.3.2
net_connect			3.44
nis_server			23.4.3
ppm	48012	3884	23.4.3
prediction_engine			23.4.3
qos_processor			23.4.3
rsp			5.59
sla_engine			23.4.3
spectrumgtw			20.41
spooler	48001		23.4.3
telemetry			23.4.0
usage_metering			9.4.2
wasp			23.4.3
webgtw			23.4.3

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

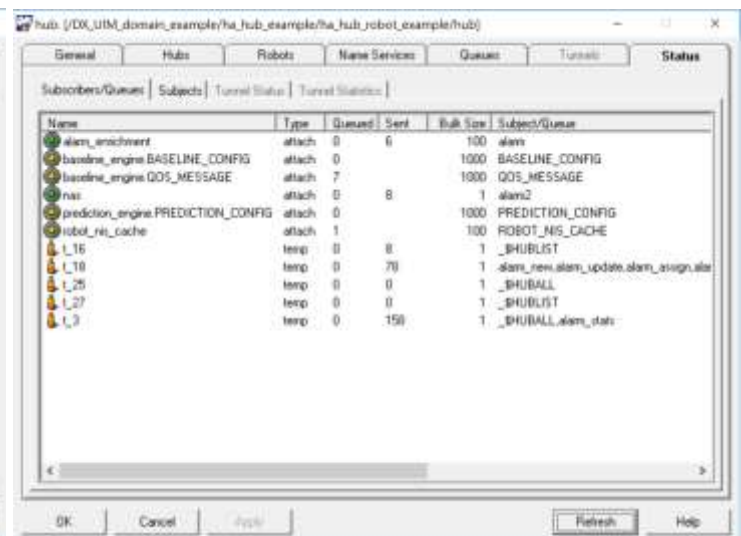
- For Secondary hub queues that don't already exist, recreate, or copy the related queues defined in the hub *postroute* section at ...[\Nimsoft\hub\hub.cfg](#) on your Primary hub, **TO** your Secondary (HA) hub, but keep most of the queues *inactive*. Then Rt-click and restart the HA hub. Shown below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

Primary hub queues (Pre-failover)

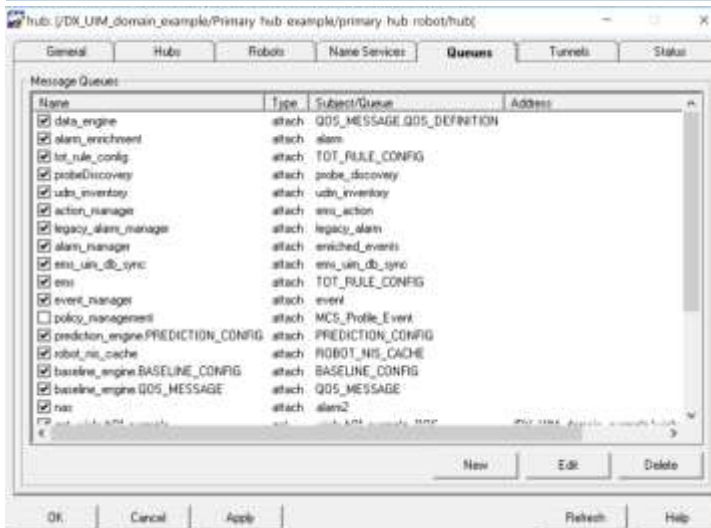
Secondary (HA) hub queues (Pre-failover)



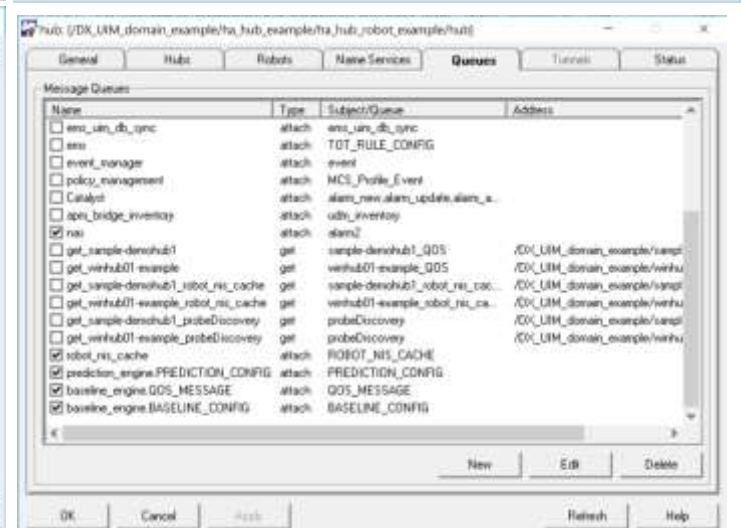
Name	Type	Queue	Serial	Bulk Size	Subject/Queue	Id
action_manager	attach	0	17		event_action	action_manager
alarm_enrichment	attach	0	0	100	alarm	alarm
alarm_manager	attach	0	24	200	enriched_events	alarm_manager
baseline_engine.BASELINE_CONFIG	attach	0	0	1000	BASELINE_CONFIG	baseline_engine
baseline_engine.QOS_MESSAGE	attach	0	0	1000	QOS_MESSAGE	baseline_engine
data_engine	attach	12	1216	1750	QOS_MESSAGE	data_engine
event_manager	attach	0	0	100	TOT_RULE_CONFIG	event_manager
event_manager	attach	0	0	1000	event	event_manager
event_manager	attach	0	22	100	event	event_manager
get_sample_demohub1	get	0	41	1000	sample_demohub1	
get_sample_demohub1_discovery	get	0	0	1000	probeDiscovery	
get_sample_demohub1_robot_nis_cache	get	0	0	1000	sample_demohub1	
get_verhub01-example	get	0	0	1000	verhub01-example	
get_verhub01-example_discovery	get	0	0	1000	probeDiscovery	
get_verhub01-example_robot_nis_cache	get	0	0	1000	verhub01-example	
legacy_alarm_manager	attach	0	0	100	legacy_alarm	legacy_alarm
nas	attach	0	51	1	alarm2	nas
prediction_engine.PREDICTION_CONFIG	attach	0	0	1000	PREDICTION_CONFIG	prediction_engine



Name	Type	Queue	Serial	Bulk Size	Subject/Queue	Id
alarm_enrichment	attach	0	0	100	alarm	alarm
baseline_engine.BASELINE_CONFIG	attach	0	0	1000	BASELINE_CONFIG	
baseline_engine.QOS_MESSAGE	attach	0	0	1000	QOS_MESSAGE	
nas	attach	0	8	1	alarm2	
prediction_engine.PREDICTION_CONFIG	attach	0	0	1000	PREDICTION_CONFIG	
robot_nis_cache	attach	1	0	100	ROBOT_NIS_CACHE	
t_16	temp	0	8	1	_BHUBLIST	
t_18	temp	0	70	1	alarm_new_alarm_update_alarm_assign_alarm	
t_25	temp	0	0	1	_BHUBLIST	
t_27	temp	0	0	1	_BHUBLIST	
t_3	temp	0	150	1	_BHUBLIST_alarm_stats	



Name	Type	Subject/Queue	Address
data_engine	attach	QOS_MESSAGE.QOS_DEFINITION	
alarm_enrichment	attach	alarm	
tot_rule_config	attach	TOT_RULE_CONFIG	
probeDiscovery	attach	probeDiscovery	
udm_inventory	attach	udm_inventory	
action_manager	attach	event_action	
legacy_alarm_manager	attach	legacy_alarm	
alarm_manager	attach	enriched_events	
event_manager	attach	event	
event_manager	attach	event	
policy_management	attach	MCS_Profile_Event	
prediction_engine.PREDICTION_CONFIG	attach	PREDICTION_CONFIG	
robot_nis_cache	attach	ROBOT_NIS_CACHE	
baseline_engine.BASELINE_CONFIG	attach	BASELINE_CONFIG	
baseline_engine.QOS_MESSAGE	attach	QOS_MESSAGE	
nas	attach	alarm2	



Name	Type	Subject/Queue	Address
event_manager	attach	event	
policy_management	attach	MCS_Profile_Event	
nas	attach	alarm2	
get_sample_demohub1	get	sample_demohub1_QOS	/DX_UIM_domain_example/sample_demohub1
get_verhub01-example	get	verhub01-example_QOS	/DX_UIM_domain_example/sample_verhub01
get_sample_demohub1_robot_nis_cache	get	sample_demohub1_robot_nis_cache	/DX_UIM_domain_example/sample_verhub01
get_verhub01-example_robot_nis_cache	get	sample_demohub1_robot_nis_cache	/DX_UIM_domain_example/sample_verhub01
get_sample_demohub1_probeDiscovery	get	probeDiscovery	/DX_UIM_domain_example/sample_verhub01
get_verhub01-example_probeDiscovery	get	probeDiscovery	/DX_UIM_domain_example/sample_verhub01
robot_nis_cache	attach	ROBOT_NIS_CACHE	
prediction_engine.PREDICTION_CONFIG	attach	PREDICTION_CONFIG	
baseline_engine.QOS_MESSAGE	attach	QOS_MESSAGE	
baseline_engine.BASELINE_CONFIG	attach	BASELINE_CONFIG	

Besides the hub *postroute* section, you can also copy the hublist section which contains all hubs that the Primary communicates with, but before you copy it, examine it first to make sure you delete the ha hub section since that would be redundant on the local HA hub.

Secondary (HA) Hub queues post failover

hub: [/DX_UIM_domain_example/ha_hub_example/ha_hub_robot_example/hub]

Name	Type	Queued	Sent	Bulk Size	Subject/Queue	Id
action_manager	attach	0	4		ems_action	action_manager
alarm_enrichment	attach	0	14	100	alarm	alarm
alarm_manager	attach	0	8	200	enriched_events	alarm_manager
baseline_engine.BASELINE_CONFIG	attach	0	0	1000	BASELINE_CD...	baseline_engine
baseline_engine.QOS_MESSAGE	attach	0	19	1000	QOS_MESSAGE	baseline_engine
data_engine	attach	0	17	100	QOS_MESSAGE...	data_engine
ems	attach	0	0	100	TOT_RULE_C...	ems
ems_uim_db_sync	attach	0	0	1000	ems_uim_db_sy...	ems_uim_db_sy...
event_manager	attach	0	6	100	event	event_manager
get_sample-demohub1	get	0	9	1000	sample-demohu...	
get_sample-demohub1_robot_nis_cache	get	0	0	1000	sample-demohu...	
get_winhub01-example	get	0	0	1000	winhub01-exam...	
get_winhub01-example_robot_nis_cache	get	0	0	1000	winhub01-exam...	
legacy_alarm_manager	attach	0	0	100	legacy_alarm	legacy_alarm_...
nas	attach	0	14	1	alarm2	nas
prediction_engine.PREDICTION_CONFIG	attach	0	0	1000	PREDICTION_...	prediction_engine
probeDiscovery	attach	0	1		probe_discovery	discovery_server
qos_processor_qos_baseline	attach	0	0	100	QOS_BASELINE	

hub: [/DX_UIM_domain_example/ha_hub_example/ha_hub_robot_example/hub]

Name	Type	Subject/Queue	Address
<input checked="" type="checkbox"/> data_engine	attach	QOS_MESSAGE.QOS_DEFINITI...	
<input checked="" type="checkbox"/> alarm_enrichment	attach	alarm	
<input checked="" type="checkbox"/> tot_rule_config	attach	TOT_RULE_CONFIG	
<input checked="" type="checkbox"/> probeDiscovery	attach	probe_discovery	
<input checked="" type="checkbox"/> udm_inventory	attach	udm_inventory	
<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 checked="" type="checkbox"/> ems_uim_db_sync	attach	ems_uim_db_sync	
<input checked="" type="checkbox"/> ems	attach	TOT_RULE_CONFIG	
<input checked="" type="checkbox"/> event_manager	attach	event	
<input type="checkbox"/> policy_management	attach	MCS_Profile_Event	
<input checked="" type="checkbox"/> nas	attach	alarm2	
<input checked="" type="checkbox"/> get_sample-demohub1	get	sample-demohub1_QOS	/DX_UIM_domain_example/sampl
<input checked="" type="checkbox"/> get_winhub01-example	get	winhub01-example_QOS	/DX_UIM_domain_example/winhu
<input checked="" type="checkbox"/> get_sample-demohub1_robot_nis_cache	get	sample-demohub1_robot_nis_cac...	/DX_UIM_domain_example/sampl
<input checked="" type="checkbox"/> get_winhub01-example_robot_nis_cache	get	winhub01-example_robot_nis_ca...	/DX_UIM_domain_example/winhu

- **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 (HA) 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, or discovery messages, 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 successfully connect to the LDAP server. Test the connection from the HA hub GUI-> General tab-> Settings-> LDAP.

- **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 net_connect is deployed to perform 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.

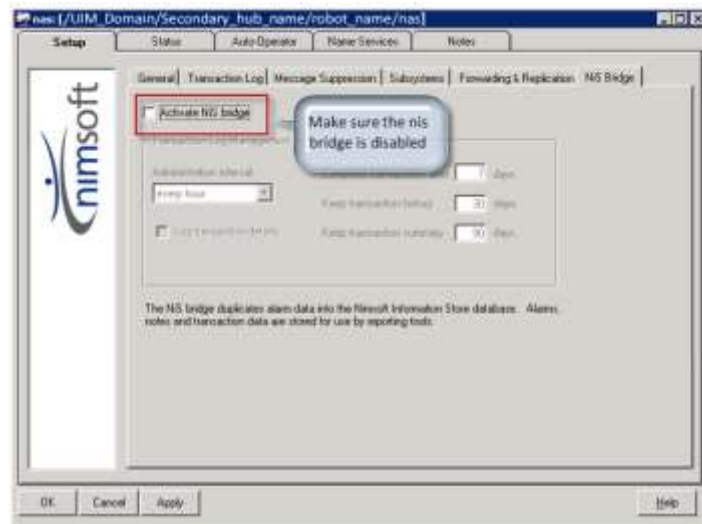
- **Gateway probes**

Lastly, on the Secondary (HA) hub, check the configuration and test connectivity for any gateway probes, e.g., sdgtw, spectrumgtw, etc., that you may already have deployed, configured 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

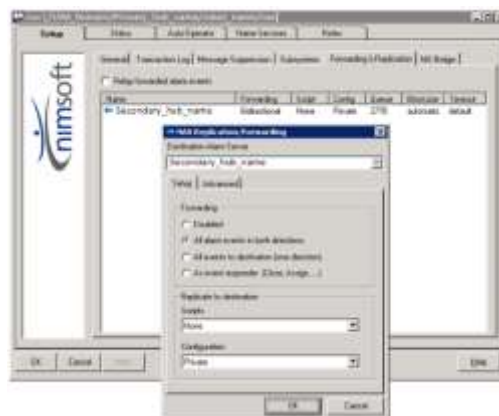
On the **Secondary** (HA) hub, nas probe configuration, Disable the nas NiS Bridge. In the nas Raw Configuration (**nis_bridge** = no). Note that only 1 NAS can update the UIM backend database tables with alarms via the NiS Bridge, so do NOT enable the nas NiS bridge on the HA hub, as this will result 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

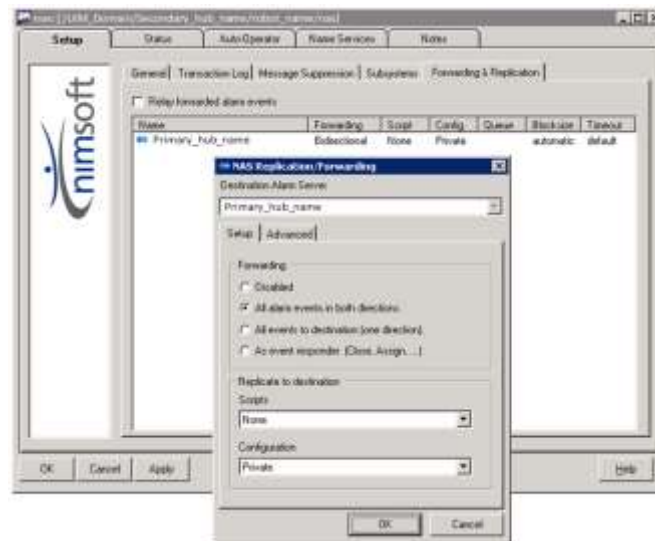
On the **Primary** hub, nas probe GUI configuration Tab: "Forwarding & Replication" - RT-click in the window to create a new NAS Forwarding & Replication rule TO the Secondary hub.

- Set the Destination Alarm Server (Secondary Hub hostname)
- Forwarding: Select All alarm events in both directions
- Select "None" for Scripts
- Select "Private" for Configuration
- Click Ok and then Click Apply, Yes to restart, then click Ok



On the **Secondary (HA) hub**, enable a Forwarding & Replication rule TO the Primary hub

- 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 probe instances.

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`

Save the original nas.cfg to a safe location first.

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

Remember, 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

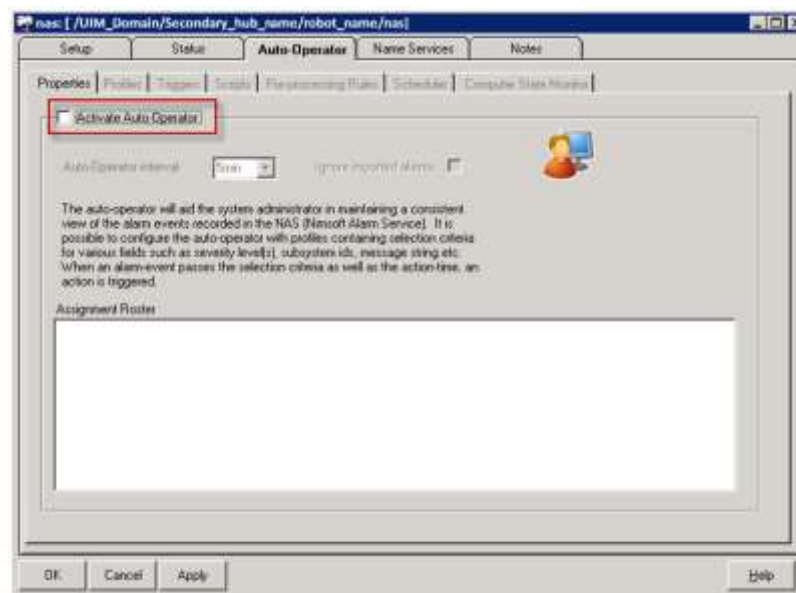
4. Open the nas probe on either hub and you should now be able to successfully add a new nas replication and forwarding entry without any popup error and continue with the HA configuration

Relay forwarded alarm events (optional)

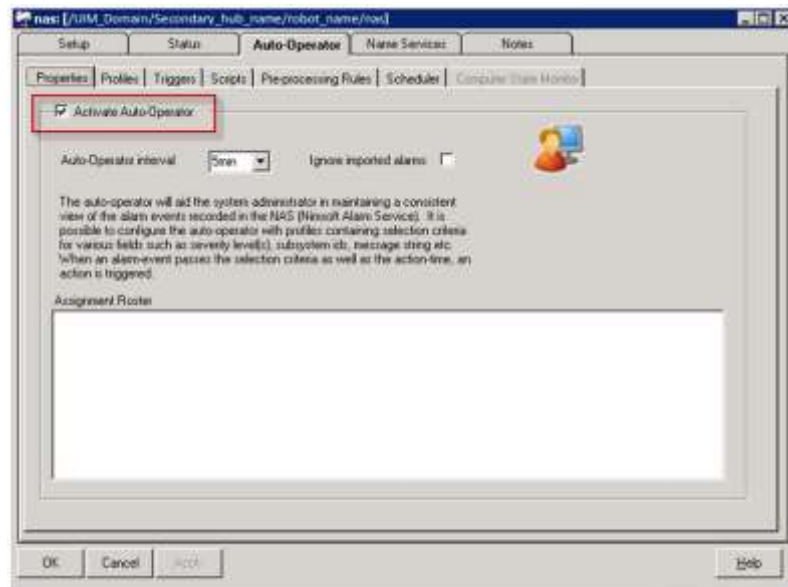
Checking the "Relay forwarded alarm events" option, alarms received from a remote nas will be forwarded.

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 to avoid 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 on the Secondary (HA) hub with AO disabled, after fallback to the Primary has occurred.



The screenshot 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
HC29001758-04257	Replication services failed for alarm server 'Primary_hub_name', reattempting.	10	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>
```

2. **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 the nas using Raw Configure mode.

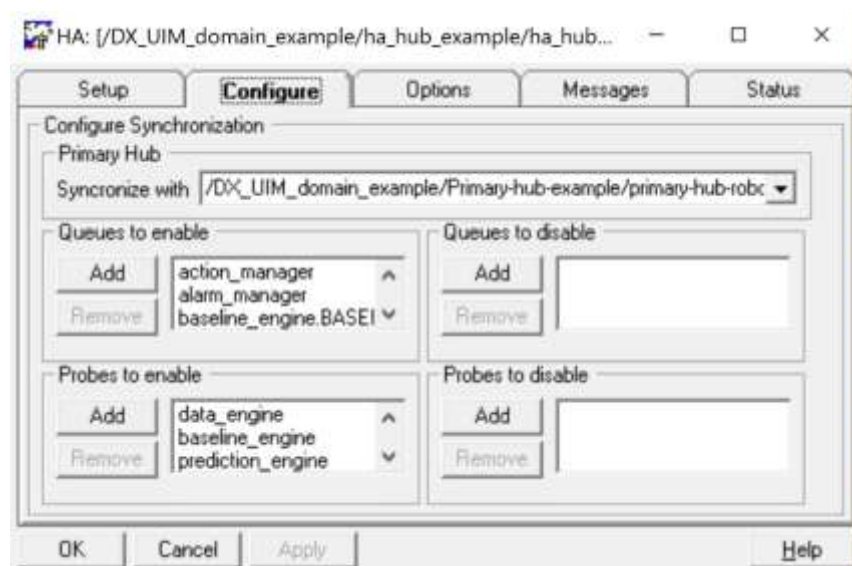
Scripts folder

The nas Scripts folder (entire contents or specific scripts) should be manually copied from the Primary hub nas to the Secondary (HA) hub nas, essentially replacing the Scripts folder and contents there.

WARNING: 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

- Download, import and 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.
- Under the Configure Tab and select the correct Primary hub NimBUS address in the 'Synchronize with' dropdown window.



Queues to enable

The HA probe allows you to 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 when viewing via Raw Configure mode:

```
<queue_up>
  queue_0 = action_manager
  queue_1 = alarm_enrichment
  queue_2 = alarm_manager
  queue_3 = baseline_engine.BASELINE_CONFIG
  queue_4 = baseline_engine.QOS_MESSAGE
  queue_5 = data_engine
  queue_6 = ems
  queue_7 = ems_uim_db_sync
  queue_8 = event_manager
  queue_9 = legacy_alarm_manager
  queue_10 = nas
  queue_11 = prediction_engine.PREDICTION_CONFIG
  queue_12 = probeDiscovery
  queue_13 = sample-demohub01_dis
  queue_14 = sample-demohub1_robot_nis_cache
  queue_15 = tot_rule_config
  queue_16 = 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 = baseline_engine
  probe_2 = prediction_engine
  probe_3 = emailgtw
  probe_4 = discovery_server
  probe_5 = ems
```

```

probe_6 = maintenance_mode
probe_7 = mon_config_service
probe_8 = qos_processor
probe_9 = sla_engine
probe_10 = spectrumgtw
probe_11 = nis_server
probe_12 = wasp
probe_13 = cdm
probe_14 = discovery_agent
</probes_up>

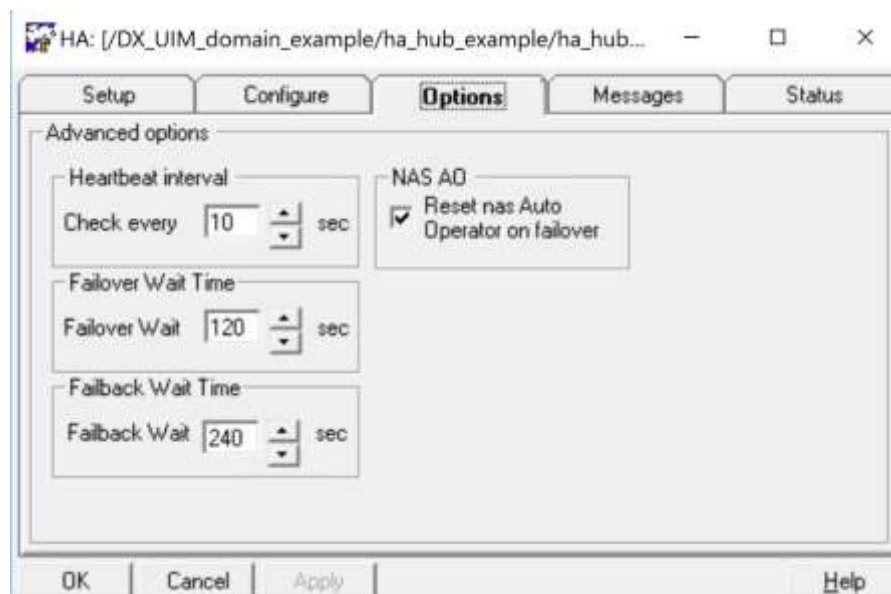
```

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

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.

Failback Wait time

How long the HA probe waits after communication with the Primary hub has been re-established

before it begins to failback,, 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 failback to the Primary.

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 also a manual task to copy / create / update your existing nas Auto-Operator (AO) profiles on the Secondary hub. You may also choose to copy and paste the relevant section(s), e.g., auto_operator, from the Primary to the HA Hub.

```
<auto_operator>
  <setup>
    interval = 5min
    active = yes
    ignore_import = no
  </setup>
  <definitions>
    <EMAIL critical (repost)>
      active = no
      action = repost EMAIL
      overdue = 5m
      level = critical
    </EMAIL critical (repost)>
    <Automatic cleanup of low-severity messages (3 days)>
      active = no
      action = close
      overdue = 3d
      level = information,warning,minor
    </Automatic cleanup of low-severity messages (3 days)>
  </definitions>
  <triggers>
    <example.network>
      active = no
      level = major,critical
      subsystems = Network
      category = example
```

```
</example.network>
<example.system>
  active = no
  level = major,critical
  subsystems = Disk,CPU,Memory,Filesystem,Process,NT-
Services,Security,Application,System
  category = example
</example.system>
<example.SLM>
```

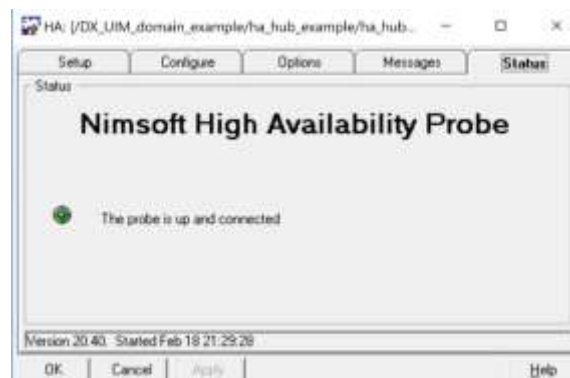
```
active = no
  sid = 1.3|1.3.*
  category = example
</example.SLM>
</triggers>
</auto_operator>
```

The same goes for the Auto Operator preprocessing rules in the filters section:

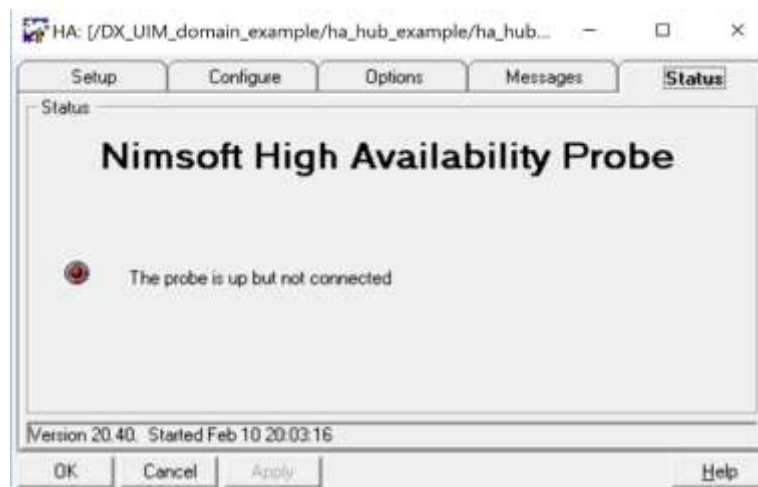
```
<filters>
  <exclude>
    <Test pre-processing rule>
      active = yes
      message_mask = /.Possible connection issue.*/
      invert = 0
      level_mask = critical
    </Test pre-processing rule>
  </exclude>
  <invisible>
    <Make old incoming alarms invisible>
      active = yes
      age = 1 day
    </Make old incoming alarms invisible>
  </invisible>
</filters>
```

At this point you can try a first-initial 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 are activated.

Note that when the Primary hub is up and running, the HA probe Status shows as **green** and displays “The probe is up and connected.”

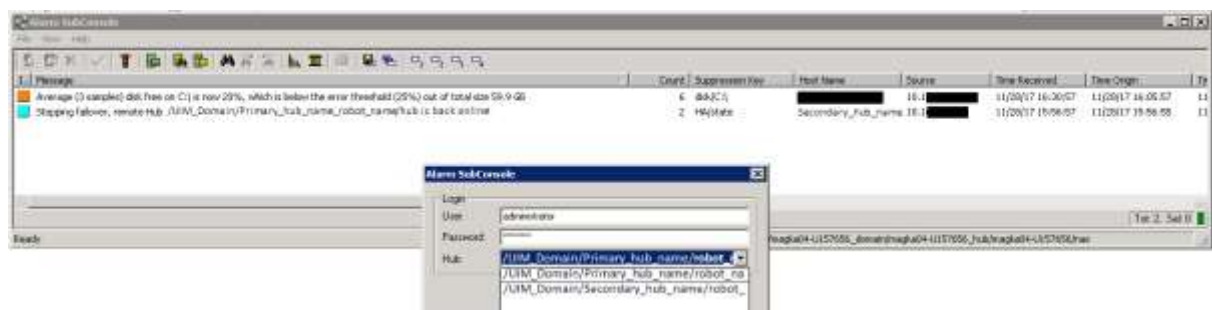


When the HA failover occurs and takes over for the Primary, the HA probe Status shows as **red** and displays “The probe is up but not connected.”



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 OC and can serve later as a backup alarm console. You can switch which hub it connects to using File->Login.

Alarm subconsole view (optional)



Activate the HA Probe

After disabling probes on the Secondary (HA) hub except for 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' (##.###.###.###)
Nov 9 15:04:06:780 HA: SREQUEST: _status ->##.###.###.###/48002
Nov 9 15:04:06:780 HA: RREPLY: status=OK(0) <-##.###.###.###/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 ##.###.###.### 48002 failed
10061
Nov 9 15:09:28:065 HA: nimNamedSession: failed to connect session to
##.###.###.###:48002 10061
Nov 9 15:09:28:065 HA: WARN: Failed to contact primary hub
'/UIM_Domain/Primary_hub_name/robot_name/hub', retry_count: 1, return_code: 2,
error_txt: communication error.
```

.....

An alarm will be generated and seen on the HA hub in the alarm subconsole window:

```
Lost contact with remote Hub
'/UIM_Domain/Primary_hub_name/robot_name/hub'
```

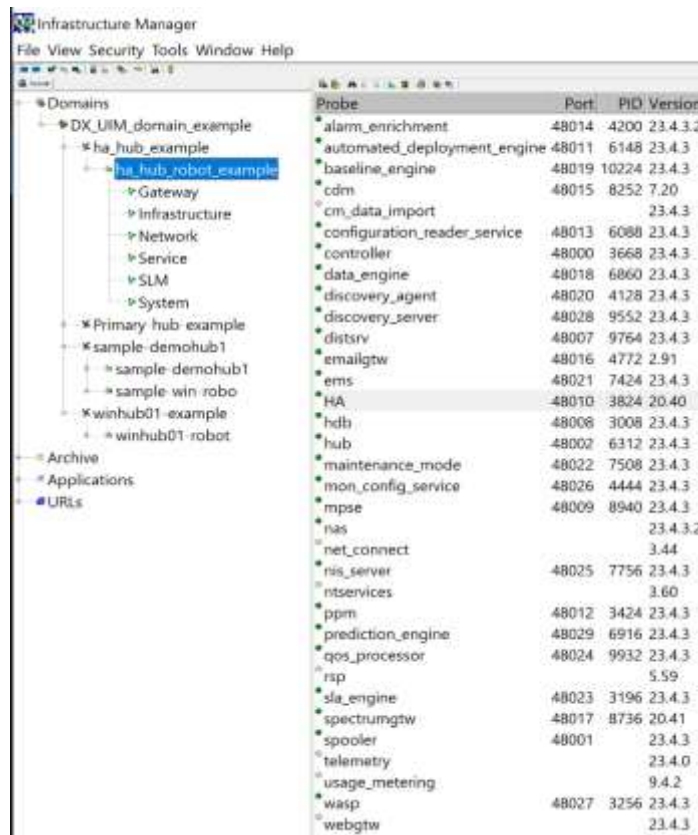
And then a subsequent alarm:

```
'Initiating failover from remote Hub'
```

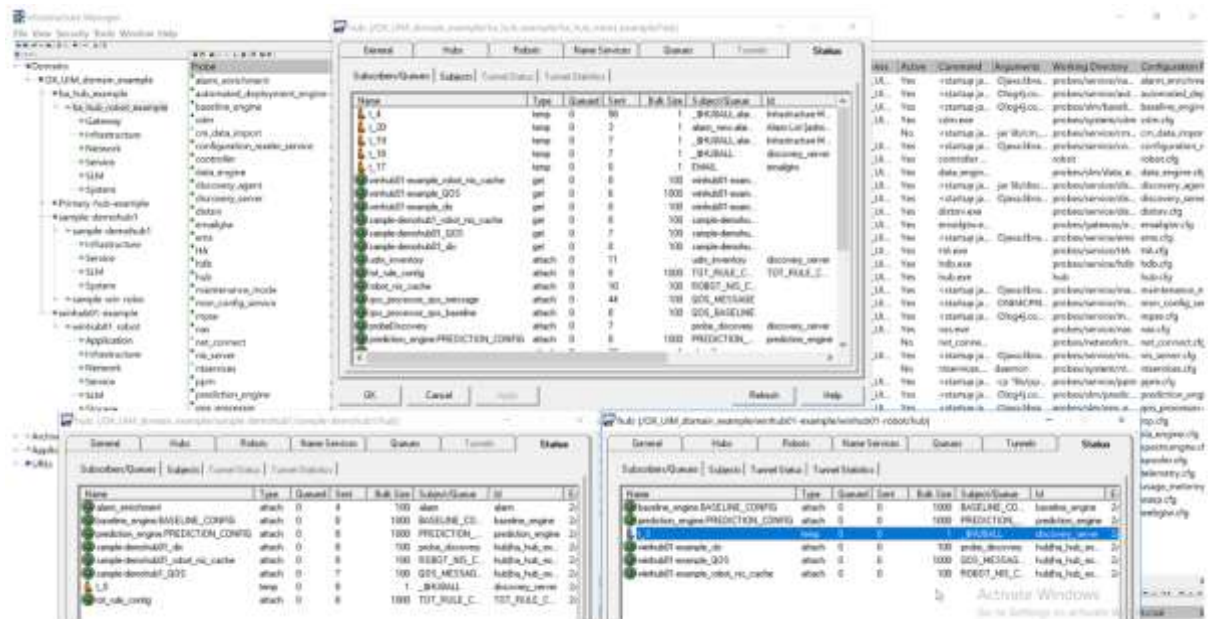
Secondary (HA) Hub post-failover

Examine failover results

Below are examples of the Secondary (HA) hub probes and queues displayed in IM after the



Probe	Port	PID	Version
alarm_enrichment	48014	4200	23.4.3.2
automated_deployment_engine	48011	6148	23.4.3
baseline_engine	48019	10224	23.4.3
cdm	48015	8252	7.20
cm_data_import			23.4.3
configuration_reader_service	48013	6088	23.4.3
controller	48000	3668	23.4.3
data_engine	48018	6860	23.4.3
discovery_agent	48020	4128	23.4.3
discovery_server	48028	9552	23.4.3
distsrv	48007	9764	23.4.3
emailgtw	48016	4772	2.91
ems	48021	7424	23.4.3
HA	48010	3824	20.40
hdb	48008	3008	23.4.3
hub	48002	6312	23.4.3
maintenance_mode	48022	7508	23.4.3
mon_config_service	48026	4444	23.4.3
mpse	48009	8940	23.4.3
nas			23.4.3.2
net_connect			3.44
nis_server	48025	7756	23.4.3
ntservices			3.60
ppm	48012	3424	23.4.3
prediction_engine	48029	6916	23.4.3
qos_processor	48024	9932	23.4.3
rsp			5.59
sla_engine	48023	3196	23.4.3
spectrumgtw	48017	8736	20.41
spooler	48001		23.4.3
telemetry			23.4.0
usage_metering			9.4.2
wasip	48027	3256	23.4.3
webgtw			23.4.3



The Primary hub was taken down during testing, and the Secondary (HA) hub successfully took over and all message queues from the hubs that were reporting to the Primary successfully switched over to the Secondary (HA) Hub.

Secondary (HA) hub probe status after fallback

When the Primary Hub recovers/returns to operation, the Secondary (HA) hub will recognize it and fallback to the Primary and the probes and queues you originally set to be enabled will update their status and show as deactivated/disabled (turn grey) in the Infrastructure Manager (IM).

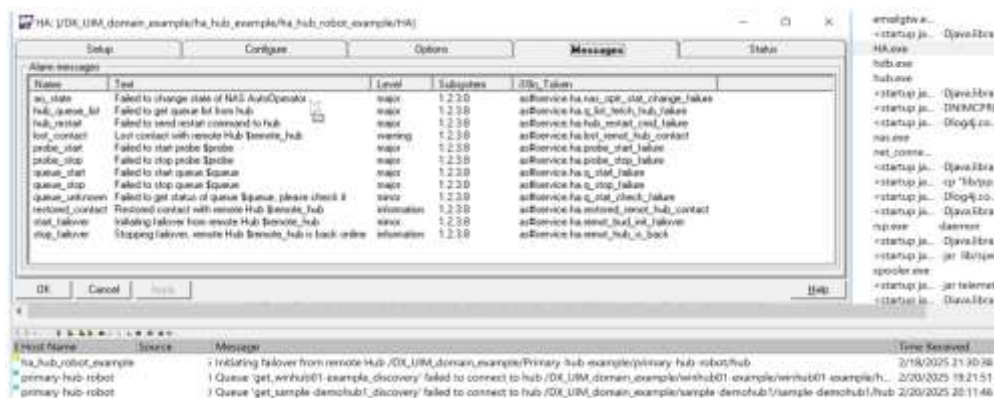
The HA.log will contain a message regarding fallback:

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

Please be aware that HA alarms do **NOT** clear automatically.



On fallback to the Primary, it may take a few minutes 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.

As mentioned previously, 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 (HA) 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 on the HA hub. 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 within the configured time
 - Enable/disable probes and queues (configurable)
- Resumes its checking of the Primary, e.g., every n 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??? Does this work or not? It doesn't seem to when configured.**

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 its paired ATTACH queue.

HA probe queue activation settings

Via Raw configure mode, the parameter `queue_activate_method` can be set to either 'queue_active' or 'postroute.' For these test scenarios, `queue_active` was used.

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

[High Availability](#)

Testing HA Failover and Troubleshooting

Test Environment:

- DX UIM v23.4.3
- Hub 23.4.3
- Robot 23.4.3
- HA 20.40 or higher
- nas 23.4.3.2
- Database: Microsoft SQL Server 2016 SP1 Enterprise Enterprise 2016 (SP3-OD) (KB5006943) - 13.0.6404.1 (X64)
- data_engine schema version: 20.45(0)

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:
##.##.##.##
Nov 16 09:52:25:587 HA: INFO: checking connection to
'/UIM_Domain/Primary_hub_name/robot_name/hub' (##.##.##.##)
Nov 16 09:52:25:590 HA: SREQUEST: _status ->##.##.##.##/48002
Nov 16 09:52:25:593 HA: RREPLY: status=OK(0) <-##.##.##.##/48002 h=37 d=294
Nov 16 09:52:25:593 HA: sockClose:0000000000B7B200:##.##.##.##/64029
Nov 16 09:52:25:593 HA: SREQUEST: _close ->##.##.##.##/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 failback
wait_time: 60
Nov 16 09:53:25:595 HA: INFO: Failback wait time expired. Continuing with
failback 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 can login via IM TO the Secondary (HA) hub. If you have the web-based admin console setup on the Secondary (HA) Hub, you can also access it via a browser at: http://<HA_hub_hostname_or_IP>/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 heartbeat check 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 the IP address 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 script 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.

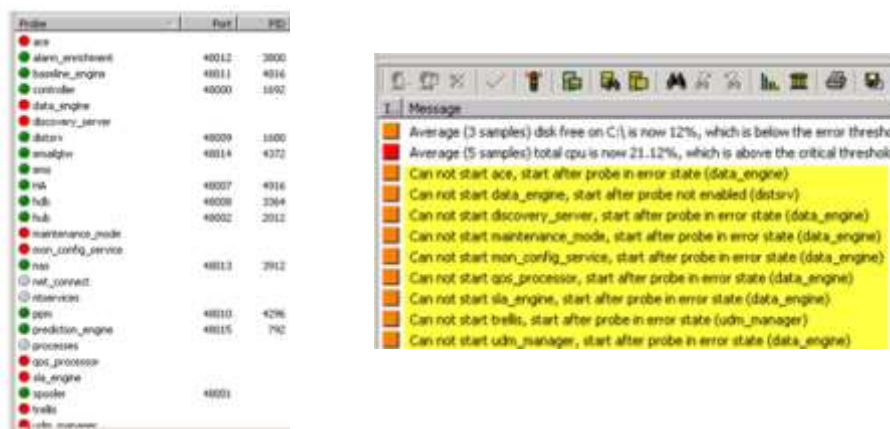
Enrichment

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).

Common problem on setup-> Probes turn red on the Secondary

If you don't 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 "Can not start" alarms will no longer occur.

Problem: HA probe throws permission denied(6) error upon failover

HA: RREPLY: status=permission denied(6) <-###.###.###.###/48002 h=37 d=0 fd=364

KB Article:

[HA failover permission denied error](#)

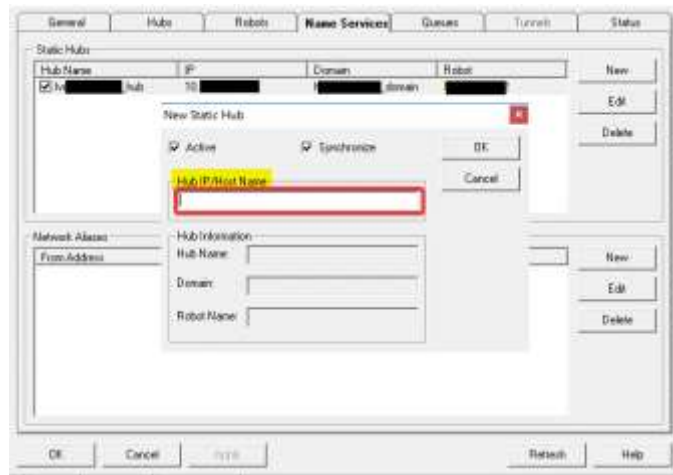
HA Best Practices

- ☐ Logging
Via Raw Configure mode, configure the Secondary hub HA, hub, robot and wasp probes with loglevel 5 and a logsize of 20000 so that while you're testing failover you can reference any activity or issues that may arise.
- ☐ Full or Partial Monitoring
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 just like the Primary hub upon HA failover. In other words, you may choose to enable a subset of the probes, monitor fewer hubs/robot systems or targets, or use less frequent polling during failover.

- ☐ **IM Version**
Install the appropriate version of the 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 but it needs to be the same IM version as the DX UIM server.
- ☐ **Admin Console state**
Confirm that you can run the Admin Console application from the Secondary hub as well when the Primary is down.
- ☐ **QOS Traffic**
If not present already, deploy at least one cdm probe and enable some QOS on each when setting up HA so you have some QOS messages flowing (especially in a Test/DEV environment where you are setting up the queues for the first time, otherwise once in a while you may see queue icons turn yellow with no traffic.
- ☐ **Probe versions**
Check to make sure that the version of each probe on the Primary matches each of the probes on the Secondary (HA) node
- ☐ **Nas NiS Bridge**
IMPORTANT! – The nas NiS bridge can only be active on one nas probe instance at a time
- ☐ **Length of Time**
HA should generally be used when the primary is down for short time periods, e.g., no more than 1-2 or maybe 3 hours maximum downtime. Otherwise, queues may become severely backed up and take more time to clear, and that includes replication queues as well, e.g., *“Replication queue for 'Primary-hub-example', has 4840 items.”*
An alternative, preferred, more heavy-duty failover solution we recommend is Microsoft Cluster Server (MSCS).
- ☐ **Queue Names (ATTACH and GET)**
In any UIM environmet you must decide upon your queue naming syntax and what is included in the name but dont make it too long. Also its a best practice to write down the attach and get queue pairs before configuring them so you dont make any mistakes, otherwise the queues wont line up logically and you might have to recreate one or more of them.
- ☐ **Backup!**
Once HA configuration is completed and working as expected, backup/SNAPSHOT VMs and safeguard all HA-setup related configuration files from the Secondary hub, HA.cfg, nas.cfg, hub.cfg, robot.cfg, data_engine.cfg, nas, etc.

☐☐

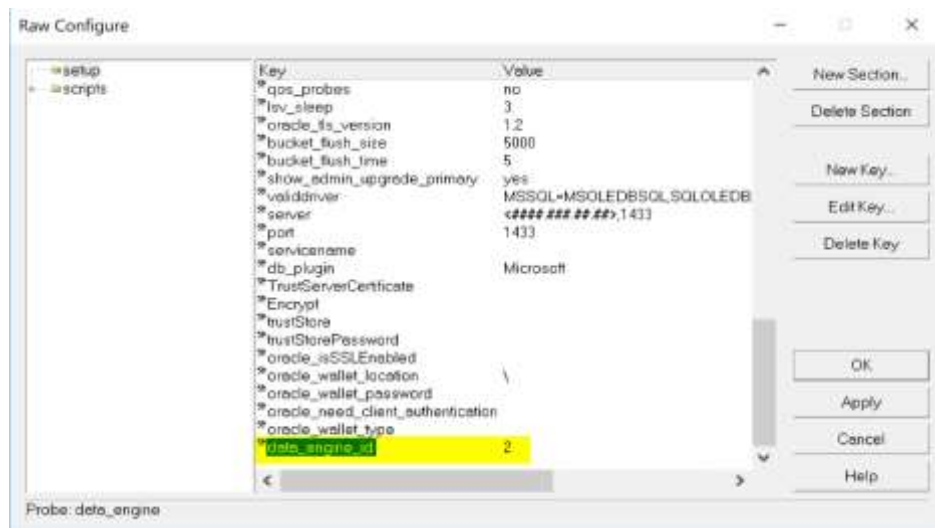
- In general, we recommend that no 'monitoring' probes are present on either the Primary or Secondary hubs, just the *core* infrastructure probes, unless it is required for some reason. If using hub Name Services you can add Static hub entries (IP address) for the remote hubs TO the Primary and Secondary (HA) hub via the hub Name Services, and add entries for the Primary and Secondary (HA) hubs TO the remote hubs via hub Named Services as well if they have any trouble reaching each other on the same network but different subnet.



- Upgrading your Primary Hub and Operator Console
 - When upgrading your Primary Hub and OC, if there is an HA probe on a designated Secondary (HA) hub in the UIM environment, make sure that you DISABLE that HA probe so that the failover hub does not takeover for the Primary during the upgrade process. Once the Primary hub upgrade is completed, consult this HA guide on options for upgrading the HA hub. Once completed, then the HA probe can be re-enabled.
 - The Operator Console must be upgraded to the same UIM version as the Primary.
 - It is a good practice to reboot both the Primary hub and the OC Robot when the hub upgrades have been completed before configuring HA.
 - A reboot is also recommended after upgrading the Infrastructure Manager (IM).
 - Rt-click and choose 'Run as Administrator' when installing/upgrading the Primary hub, Operator Console or IM (NimBUSManager.exe).

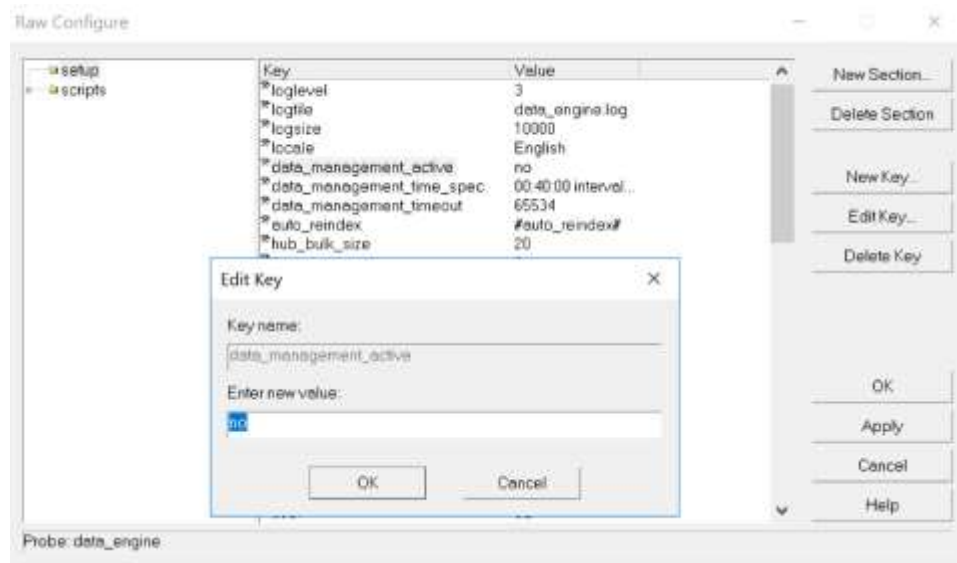
data_engine (Primary versus Secondary mode)

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 `data_engine_id` setting determines the data_engine's role as Primary or Secondary. 1 indicates its the Primary and 2 is for the Secondary (HA) hub (see below). Note that data_engine *maintenance* should always be disabled on the Secondary, e.g., `data_management_active = no`.



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 the HA hub generates will use 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/monitoring 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 origin info 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.**
- The **data_engine_id** does **NOT** change on failover and/or failback. The data_engine id on the Primary hub should always be set to 1, Secondary (HA) hub remains set to 2.

```
select * from tbn_de_controller
```

Id	SPId	Address	State	TimeRegister	TimeRegister
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 OC availability/failover

DX Infrastructure Manager (UIM), does not currently test nor support OC High availability/failover. If the primary hub fails, you need to manually point wasp to the HA hub as there is no supported automatic OC failover.

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

That stated, for field-developed probes/scripts that can be leveraged for successful OC 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 v20.4 or higher versions when implementing OC failover, you must **ensure you copy the cryptkey from the Primary hub to any OC node(s)**.

Copy the original certificate.pem over from the Primary to the Secondary (HA) hub directly. (do not try to copy/paste the file contents). 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 an article regarding the loss of child hubs upon failover.

[Upon HA hub failover, secondary remote hubs did not switch over as expected](#)

Notes on deploying spectrumgtw

Prerequisites- ensure that you have the following probe versions:

- nas – 23.4.3.2
- EMS probe – 23.4.3
- spectrumgtw – 20.41
- HA probe – 20.40

Operator Console (OC) Robot

- webservices_rest 23.4.3
- UIMAPI 23.4.3

The ems probe is HA aware/compliant for failover. 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 to true. When the failover happens and ems is running on the Secondary (HA) hub, the parameter ‘isprimary = false’.

Before deploying spectrumgtw, perform a round of failover of the UIM Hub and failback to see whether UIM alarms are generated and the UIM inventory is intact and operating as expected.

spectrumgtw deployment steps

1. Deploy the spectrumgtw probe to the Primary and the HA hub

2. Add spectrumgtw to the probes to enable the section and `ems_uim_db_sync` in the queues to enable both of those sections in the HA probe
3. Rt-click and restart the HA probe
4. On the Primary hub, Activate spectrumgtw and Deactivate spectrumgtw on the HA hub.
5. Open the Admin Console and launch the Configuration page and choose configure spectrumgtw. Ensure that you provide HA Probe Robot Address [/Domain_name/hub_name/robot_name] in the Probe Setup section.

Probe Setup

Log level *	3 - Info	▼
Is Primary *	True	▼
HA Probe Robot Address	Enter HA Probe Robot Address 	
Specify the Robot Address where HA Probe installed: /Domain_name/hub_name/robot_name		

See the spectrumgtw documentation for further configuration.

[Spectrumgtw AC configuration](#)

6. Select Save, which allows spectrumgtw to collect the HA hub status before integrating with Spectrum.
7. Copy the spectrumgtw.cfg file from the Primary hub to the HA hub.
8. Open the spectrumgtw.cfg file in the HA hub, and change the “isPrimary = false” attribute to true

Key points to note:

When the spectrumgtw is active on the HA hub and the nas NiS-bridge is disabled on the Secondary (HA) nas, then the nas alarms that are created or updated are not reflected in Spectrum. **These alarms sync only after a failback to the Primary hub.** Alarms that are purposely being routed to EMS continue to synchronize between UIM and Spectrum. If any UIM alarm is cleared in Spectrum or a Spectrum alarm is cleared in UIM during a failover or a failback, while the spectrumgtw is Activated, then those alarms get recreated. If UIM alarms are cleared in UIM or Spectrum alarms are cleared in Spectrum, then these alarms are not recreated.

Lastly, note that the `webservices_rest` package is a prerequisite for the spectrumgtw so it must be deployed on the OC Robot(s) for the spectrumgtw to work as expected upon failover of the Primary hub.

Notes when rebooting the Primary Hub:

When the Secondary (HA) hub has fully taken over for the Primary hub, if you reboot the Primary, the HA cannot reach the Primary over the network using the HA 'heartbeat' method so the HA doesn't take over - until the Primary comes back up again and the hub-robot is running, then if its stopped or some issue causes the Primary hub-robot to fail, failover to the HA Hub can occur once again.

When the Primary is up and running normally you see this in the Secondary hub's HA.log:

```
HA: INFO: UpdateCache - updated remote hub information: <primary_ip_address>
Feb 21 15:35:20:806 2 HA: INFO: checking connection to
'/DX_UIM_domain_example/Primary-hub-example/primary-hub-robot/hub'
(<primary_ip_address>)
Feb 21 15:35:20:806 4 HA: CONNECT: 000002D6A89A3150(504)
<secondary_ha_ip_address>/58175-><primary_ip_address>/48002
```

When the HA hub cannot reach the Primary you see these entries in the HA.log:

```
Feb 21 15:36:21:873 2 HA: sockConnect - connect to <primary_ip_address> 48002
failed 10061 (sfd=288)
Feb 21 15:36:21:873 1 HA: nimNamedSession: failed to connect session to
<primary_ip_address>:48002 10061
Feb 21 15:36:21:873 0 HA: WARN: Failed to contact primary hub
'/DX_UIM_domain_example/Primary-hub-example/primary-hub-robot/hub', retry_count:
0, return_code: 2, error_txt: communication error.
```

HA.log during/after the reboot shows:

```
HA: INFO: FAILOVER: 'wait_time' has expired. Checking for state change.
Feb 21 16:20:42:181 4 HA: ciClose - [C9F43F4F8D8B8D346647F5F3B6D7BE0DA]
Feb 21 16:20:46:183 3 HA: INFO: Calling UpdateCache(0)
Feb 21 16:20:46:183 4 HA: INFO: ENTER: UpdateCache: force: 0
Feb 21 16:20:46:183 4 HA: INFO: gszRemoteHub: /DX_UIM_domain_example/Primary-
hub-example/primary-hub-robot/hub
Feb 21 16:20:46:183 4 HA: CONNECT: 000002D6A890C870(876)
<secondary_ha_ip_address>/60964-><secondary_ha_ip_address>/48000
Feb 21 16:20:46:183 3 HA: SREQUEST: nametoip -><secondary_ha_ip_address>/48000
```

Then it failsback/falls-back to the Primary Hub:

...but note that after the reboot the hub/controller is automatically up and running again.

```
Feb 21 16:20:46:185 2 HA: INFO: UpdateCache - updated remote hub information:
<primary_ip_address>
Feb 21 16:20:46:185 2 HA: INFO: checking connection to
'/DX_UIM_domain_example/Primary-hub-example/primary-hub-robot/hub'
(<primary_ip_address>)
Feb 21 16:20:46:186 4 HA: CONNECT: 000002D6A890A260(916)
<secondary_ha_ip_address>/60967-><primary_ip_address>/48002
Feb 21 16:20:46:186 3 HA: SREQUEST: _status -><primary_ip_address>/48002
Feb 21 16:20:46:186 3 HA: RREPLY: status=OK(0) <-
<primary_ip_address>/48002 h=37 d=208 fd=916
Feb 21 16:20:46:186 3 HA: SREQUEST: _close -><primary_ip_address>/48002
Feb 21 16:20:46:186 0 HA: INFO: FAILBACK: Connection to
'/DX_UIM_domain_example/Primary-hub-example/primary-hub-robot/hub' restored.
Issuing state change.
```

```
Feb 21 16:24:46:188 1 HA: INFO: Changing state from 'activated' to 'deactivated'
Feb 21 16:24:46:188 1 HA: INFO: expanded 'Stopping failover, remote Hub
```

```
$remote_hub is back online' to 'Stopping failover, remote Hub
'/DX_UIM_domain_example/Primary-hub-example/primary-hub-robot/hub is back online'
Feb 21 16:20:46:186 4 HA: INFO: Enter: state_check
Feb 21 16:20:46:186 3 HA: INFO: state == '1'
Feb 21 16:20:46:186 3 HA: INFO: gConnected: 0
Feb 21 16:20:46:186 5 HA: ciOpen - cache path: C:\Program Files
(x86)\Nimsoft\niscache
Feb 21 16:20:46:186 3 HA: ciGetDeviceIdentifiers -
```

```
/DX_UIM_domain_example/Primary-hub-example/primary-hub-robot/hub found (remote device) [D34ABB363A37EA0034D1F1193101EEB4D]
Feb 21 16:20:46:186 2 HA: ciRead - reading
DEV [D34ABB363A37EA0034D1F1193101EEB4D]

Feb 21 16:20:46:187 1 HA: INFO: primary hub is back online, sleeping for failback wait_time: 240
Feb 21 16:24:46:187 1 HA: INFO: Failback wait time expired. Continuing with failback actions.
Feb 21 16:24:46:187 1 HA: INFO: expanded 'Restored contact with remote Hub $remote_hub' to 'Restored contact with remote Hub
/DX_UIM_domain_example/Primary-hub-example/primary-hub-robot/hub'
```

Lastly, when the Primary is stopped or fails for any reason once again, e.g., hub is stopped, robot is hung, etc., if its stopped or any issue causes the Primary hub-robot to fail, failover to the HA Hub can occur once again.

FAQs

1. In an HA environment, what other configurations 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 their 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. For nas/ems, on a failover event, will the HA node/secondary be able to keep alarms in sync out of the box?

Yes, but you must configure bidirectional nas forwarding & replication as described in this guide.

3. Any risks/disadvantages in HA operation?

There are a few disadvantages for instance, OC failover and CABI (bundled) operation upon failover are not 'officially' supported/tested but there are some posts in the UIM community on how to achieve CABI failover using the HA probe and they are reported to be successful.

4. Are there other failover alternatives?

Ideally, we recommend using Microsoft Cluster Server (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](#)