Infoblox
CONTROL YOUR NETWORK

Network Automation Operations Center –
Replacement and Failover Procedures

29 July 2015

Replacement and Failover Overview

Operations Center (OC) customers may need to replace appliances (either the OC itself, or a collector) for a variety of different reasons: to go to a newer hardware version; to install hardware with more capacity; or because of a hardware failure. For customers with stand-alone appliances, this process is fairly straightforward, however, for the OC customers there are many factors that need to be taken into account.

The replacement can be done using a new system shipped from Infoblox, or from a spare appliance that the customer has already pre-positioned, or from a system the customer has already licensed and configured. With each of the choices there are increasing levels of complexity, as described below.

The most common approach is a replacement based upon a Returned Material Authorization (RMA), or a hardware upgrade purchase. While this might take a bit longer, due to the time to ship and configure the new system, this is often the most straightforward option.

Some customers choose to purchase spare appliances and have them pre-positioned at their locations. This can reduce time to restore, but brings on a few management questions that the customer must consider. For example, often an OC/collector deployment uses two different models of hardware – so the plan must account for that aspect. Other factors to consider include the NetMRI licensing model, and the version upgrade-path.

More complex than a simple replacement is a failover arrangement. Rather than simply replacing an existing piece of hardware, the customer may choose to failover to a second piece of hardware that is on-line in parallel to the primary. For the purpose of this document, a “replacement” assumes all the characteristics of the system it replaced (e.g. IP address) whereas failover system will have some unique elements (e.g. a different IP address and hostname).

Terminology

There are four different categories that can be considered for replacement/sparing or failover activities:

- Returned Material Authorization (RMA) – Once it is determined that a replacement is needed, new hardware, and a new license, is shipped from Infoblox or a world-wide depot that serves the customers location. Upgraded hardware purchases also fall under this heading, procedurally.
- “On-Site Hardware (OSH)” – Customer purchases hardware, in advance, to hold in their inventory, thus avoiding shipping time of an RMA situation. However, the customer will still need to obtain a new license for the hardware at the time that hardware is put into use (for all other intents and purposes an OSH and an RMA procedure are identical). This is a hardware purchase only, and the hardware for OSH is priced at the same level as primary systems. Note: previously the term On-Site Spare was used to describe this approach, but it has been changed to clearly differentiate between hardware only prepositioning, and licensed spares. When talking with the account team or purchasing OSS might be recognized.
- “Redundant Licensed Spare” – This can be in one of two forms “cold-spare” or “warm-spare”. In both cases, the customer has purchased the hardware and a license in advance. The hardware is priced at the same level as OSH, above. However, the licenses (with a SKU of type “-R”) are priced at a substantial discount. These licenses are not authorized for use at the same time as the primary licenses, except during a failover transition period.
    - Cold-Spare – a parallel system where components are licensed, but not powered on. This is similar to the on-site hardware, but with licenses already generated and provided.
    - Warm-Spare – a parallel system where components are licensed, and powered on, but not configured to poll. This arrangement provides a potential basis for failover, in addition to replacement. When referring to systems use for failover purposes, the term ‘standby’ is used.
- Active/Active – While not truly a replacement/sparing approach it is included for completeness. In this case, there is a parallel system in which all components are duplicated with licensed, powered-on NetMRI components. Both systems are polling the same range of devices as the primary system. This requires two sets of hardware and full licenses. Redundant (type “-R”) licenses cannot be used.

Each of those approaches has advantages and costs (monetarily or management). From an implementation standpoint RMA and OSH can be considered as one. While cold-spare and hot-spare are the same from a licensing perspective, they need to be treated separately from an implementation perspective. The categories described in the terminology can be implemented in a number of different ways. These approaches can be blended by the customer to suit their needs.

Replacement/Failover Approaches and Plans – Operations Center

Approach one: Simple backup and restore using RMA or On-Site Hardware

- Archive the active OC DB to network storage daily or weekly (automated) or prior to the activity
- In the OSH case, purchase, rack and cable the backup hardware.
- Upon need to replace the OC:
  - RMA appliance and receive and rack replacement (not needed in OSH case).
  - Obtain and install license (should be provided with RMA, will need a support call with OSH).
  - Go through the ‘configure server’ process.
  - Upgrade to appropriate version, and install hotfixes.
  - Transfer archive from network storage, and restore archive.
  - Re-register collectors.
  - Enable collection.
- Downtime: Days (shipping, rack, license, and restore); half a day to a day with OSH.

Approach two: Licensed Spare – Cold Spare – This lends itself to replacement rather than failover

- Purchase an additional appliance and “redundant” SKUs for backup system. (Note: currently the OC license does not define a number of devices – just the OC capability – so this license is easy to manage.)
- Rack and cable the backup appliance.
- Archive the active OC DB to network storage daily or weekly (automated) or prior to the activity
- Upon need to replace the OC:
  - Bring backup OC online.
  - Go through the ‘configure server’ process and apply license.
  - Upgrade to appropriate version, and install hotfixes.
  - Transfer archive from network storage, and restore archive.
  - Re-register collectors.
  - Enable collection.
- Downtime: Several hours to half a day.
- Keeping the system up to date with versions and hotfixes can be done during windows where the system is brought on-line temporarily for upgrade/hotfix application, and then powered off again. Since the purpose of this system is replacement (same IP / hostname) it should be assigned a temporary IP during those uptimes. If this is done (the system has been given a temporary IP address), there will still be a need to configure the replacement OC with the primary’s IP address as part of the replacement activity.

Approach three: Licensed Spare – Warm Spare – This lends itself more to failover than replacement

- Purchase an additional appliance and “redundant” license SKUs for standby.
- Rack, cable, power-up, configure and license standby appliance with redundant license. As of 6.9.x/7.0.x the OC license does not define a number of devices – just the OC capability – so this is easy to manage.
- This device now will have a unique IP/Hostname, so this falls into the failover category.
- Archive the active OC DB to the warm standby server daily or weekly (automated) or prior to the activity.
- Keep standby OC up to date with upgrades/hotfixes, so it is always ready to take over in a failover case.
- Note, however, because there is no version roll-back capability, customers may want to take special consideration at the time of an upgrade. There are advantages and disadvantages to upgrading the primary system first, or the standby system first.
- Upon need to replace the OC:
  - Restore archive (this can be done with an automated script, so this system is always ready).
  - Re-register collectors to the standby system, which is now in primary role.
  - Enable collection.
  - Inform users of the new system’s IP, or update DNS.

- Downtime: An hour to several .hours
- This process can be even faster if scripts are used to push the archive data, and keep the standby system up to date with the archived data.
- There are still some rough edges in maintaining an OC as a warm standby – for example if it is configured in 6.9 without any attached collectors (which is an optimal configuration), then the system health reporting will be thrown off. The OC had not been designed to run without collectors, and this warm-standby case was not considered. This is partially addressed in 7.0.1, with additional fixes in 7.0.2.

Approach Four: Warm-Spare for entire System Failover – OC and parallel set of collectors

- Purchase additional appliances and “redundant” license SKUs for all systems.
- Rack, cable, power-up, configure and license standby appliances with redundant licenses.
- The devices now will have a unique IP/Hostname, so this falls into the failover category.
- Archive the active OC DB to the warm standby server daily or weekly (automated) or prior to the activity.
- Keep standby OC and collectors up to date with upgrades/hotfixes, so they are always ready to take over in a failover case.
- Note, however, because there is no version roll-back capability, customers may want to take special consideration at the time of an upgrade. There are advantages and disadvantages to upgrading the primary system first, or the standby system first.
- Upon need to replace OC:
  - Restore archive (this can be done with an automated script, so this system is always ready).
  - Enable collection
  - Turn off all primary collectors.
  - Inform users of the new system’s IP, or update DNS.
- Downtime: An hour to several .hours
- This process can be even faster if scripts are used to push the archive data, and keep the standby system up to date with the archived data.
- Must ensure that the primary collectors are turned off, as they could be still polling, even though the primary OC they were connected to has gone down.
- This approach has some downsides, but is possible. The principal downsides/considerations include:
  - The need to fully replicate the active system,
  - When there is a need for replacing one component (the OC) this process is actually swapping out all components. This may mask or introduce other problems
  - When configured this way, it becomes more difficult to also do failovers of individual components. If just a collector was to be failed-over, there would be extra deregistration required, etc.

Approach Five: Active/Active

- Purchase an additional appliance and full license SKUs for standby OC and all collectors
- Install and configure all.
- Prepare for certain network devices to crash under the stress of too much polling. Many network devices can handle the load, but some can’t.
- Seriously, while this would result in more license revenue for Infoblox, we don’t think this is the best approach, except in special circumstances.

Replacement/Failover Approaches and Plans – Collectors

Collector replacement strategy has a different set of complex challenges than the OC replacement. Collectors themselves are not backed up, but they are the systems that have device license limits assigned. Most of what they need is sent to them, at registration, from the OC. This process, however, still has some gaps. For example, a collector that created device IDs while running 6.8.x, that is later replace while running 6.9 (or above) will lose track of those original device IDs, and rediscover the devices using the 6.9.x device ID schema. This is handled correctly as of 6.9.4.

Approach one: Simple backup and restore using RMA or On-Site Hardware

- In the OSH case, purchase, rack and cable the backup hardware.
- Upon failure of collector:
    - RMA appliance and receive and rack replacement (not needed in OSH case).
    - Obtain and install license (should be provided with RMA, will need a support call with OSH).
    - Go through the ‘configure server’ process for the collector.
    - Upgrade to appropriate version, and install hotfixes.
    - Register the collector with the OC, following standard registration process
    - Change the serial number of the collector on the OC to indicate that the replacement unit has taken the place of the failed/replaced unit.
- Downtime: Days (shipping, rack, license, and restore); half a day to a day with OSH.

Approach two: Licensed Spare – Cold Spare – This lends itself more to replacement than failover

- Purchase an additional appliance and “redundant” SKUs for standby
- Rack and license standby appliance with redundant license. As of 6.9.x/7.0.x the collector license defines the authorized number of devices – so a collector in the ‘standby’ mode needs to have a license that is large enough to match any primary that it might be used to replace.
- Upon failure of collector:
    - Bring backup collector online
    - If the collector has been previously brought online and registered to another OC, do a factory reset, and reapply the license – Not expected in a cold-spare case, but noted here, just in case.
    - Upgrade to appropriate version, and install hotfixes.
    - Register the collector with the OC, following standard registration process.
    - Change the serial number of the collector on the OC to indicate that the replacement unit has taken the place of the failed/replaced unit.
    - Power off (admin shutdown) the original primary collector to ensure no possibility that it will keep polling.
- Downtime: Several hours to half a day.
- Note: a factory reset will erase the copy of the license that might be stored in the collector’s admin home directory. Keep a spare copy.

Approach three: Licensed Spare – Warm Spare – This lends itself more to failover than replacement

- Purchase an additional appliance and “redundant” SKUs for standby
- Rack and license standby appliance with redundant license. As of 6.9.x/7.0.x the collector license defines the authorized number of devices – so a collector in the ‘standby’ mode needs to have a license that is large enough to match any primary that it might be used to replace.
- Do not register it with any OC – get it initially configured, but stop short of registration.
    - It is better for Warm-Spare collectors to remain configured as stand-alone units until they are called into service.
    - While it needs to be licensed as a collector eventually, it is far better for it to be treated and managed as a stand-alone until such time as it is put into production.
    - If not then it assumes some characteristics that need to be factory reset prior to associating it with the production OC. Thereby requiring extra work to re-configure AND reapply the license file (which is hopefully also stored in a safe place outside of the appliance, as a factory reset will delete the copies on the appliance)

- Upon failure of collector:
  - If the collector has been previously registered to another OC, do a factory reset, and reapply the license.
  - Upgrade to appropriate version, and install hotfixes. (if it has not been kept up to date – but one advantage of warm standby is that this system can be kept up-to-date with upgrades/hotfixes)
  - Register the collector with the OC, following standard registration process
  - Change the serial number of the collector on the OC to indicate that the replacement unit has taken the place of the failed/replaced unit.
  - Power off (admin shutdown) the original primary collector to ensure no possibility that it will keep polling.
- Downtime: an hour to several hours.
- Note: a factory reset will erase the copy of the license that might be stored in the collector’s admin home directory. Keep a spare copy.

Operations Center Replacement/Failover Procedure

When you perform an OC replacement/failover, you first restore the database archive on the Replacement/Standby Operations Center, and then re-register all collectors from the Primary Operations Center to the Replacement/Standby Operations Center. The order of these operations is dependent on the situation – bringing up a cold-standby system for a replacement operation would need most of these items done in one activity. Keeping a warm-standby system available for failover would involve having several steps already completed, or occurring on a regular basis, followed by an activity to put the failover in motion.

Note: To fully configure the Standby Operations Center, you will need a second product license for the failover system with the same licensing entitlements as the Primary Operations Center license. Contact your Infoblox sales representative for more information.

Complete the following to perform a manual replacement/failover:

1. Log in to the Replacement/Standby Operations Center command line via SSH using the admin/admin system credentials.
2. Execute the following Admin Shell CLI commands on a newly installed or factory reset Standby Operations Center instance:

   ```
   admin-na206.corp100.com> license <license filename>.gpg
   ```

   (Install the license for the Standby Operations Center)

   ```
   admin-na206.corp100.com> configure server
   ```

   Define server settings for the Standby Operations Center. Make a note of your settings for Step 6 of this Procedure.

   Note: The `configure server` command also generates a new self-signed certificate for the Standby Operations Center. In cases where a CA-signed certificate is used in the original Operations Center, the HTTPS certificates need to be configured using the procedures described in the topic *Network Automation Certificate and Protocol Security* in the Admin Guide and in the online Help.

3. Verify your settings by entering the following commands:

   List the complete config settings for the Standby Operations Center.

   ```
   admin-na206.corp100.com> show settings
   ```

   Show the installed license for the Standby Operations Center.

   ```
   admin-na206.corp100.com> show license
   ```

4. Transfer the Primary Operations Center database archive to the Standby Operations Center, via SCP, if it has not already been sent there.

   Note: You can also configure the database Archive for the Primary as an automated transfer, using the Settings –> Database Settings –> Scheduled Archive screen on the Primary Operations Center to archive the OC database to the system designated as the Standby. The Archive directory in this case should be set as “Backup”; refer to the *Database Archiving Functions* topic in the product documentation for more details.

   Note: When using the automated database archiving, you must first log in to the Standby Operations Center through your web browser, and set the admin password to a value different from the “admin” factory default. In this case, after the Standby OC system is activated as the Primary, you must also go to the

Settings –> Database Settings –> Scheduled Archive tab and define another remote system to back up the new OC's database archive.

If you schedule the transfer to occur within six hours of the start of weekly maintenance, no new archive will be created. Instead, the archive generated by weekly maintenance will be used. For large deployments with a lot of data, configuring archiving to occur more frequently than the weekly interval may affect overall system performance.

5. Using the Admin Shell on the Standby Operations Center, restore the database archive on the Standby Operations Center. Restore time depends upon the size of the database, and may take several hours for a large system.

```
admin-na206.corp100.com> restore ExampleNet_4050201203200004-20130221-641
```

Note: The admin credentials (that default to admin/admin) are changed on the Standby Operations Center following the database restore operation. The Standby Operations Center will use the admin credentials that previously applied on the Primary Operations Center.

6. When the database restore task finishes on the Standby Operations Center, run **`configure server`** a second time to regenerate the Standby Operations Center's self-signed certificate for HTTPS access. Re-enter your settings previously defined in Step 2 of this Procedure.

7. In the Admin Shell on the Standby Operations Center, configure the VPN tunnel server on the Standby Operations Center using the same VPN subnet and other settings as on the Primary. When asked for the **Server Public Name or IP address**, be sure to enter the correct value for the Standby Operations Center. Do not configure a reference collector. The following listing is a sample capture for an entire session:

```
admin-na206.corp100.com> configure tunserver
+++ Configuring CA Settings
CA key expiry in days [5475]:
CA key size in bits [2058]:
+++ Configuring Server Settings
Server key expiry in days [5475]:
Server key size in bits [2048]:
Server Public Name or IP address: <new IP address for Standby>
Protocol (tcp, udp, udp6) [tcp]:
Tunnel network base [5.0.0.0]:
Block cipher:
            0. None (RSA auth)
            1. Blowfish-CBC
            2. AES-128-CBC
            3. Triple DES
            4. AES-256-CBC
Enter Choice [2]:
Use compression [y]:
```

Note: In configure server, you can optionally designate a Network Automation client system as a "reference" system that will be used as a source of common settings, but that should **NOT** be done in this procedure.

```
Enter reference system serial number or RETURN to skip: <press Enter here>
Use these settings? (y/n) [n]: y

Initializing CA (may take a minute) ...
Creating Server Params and Keypair ...
Generating DH parameters, 2048 bit long safe prime, generator 2
```

```
This is going to take a long time
....++*++*++*

+++ Creating Server Config ...
Successfully configured Tunnel CA and Server

The server needs to be restarted for these changes to take effect.
Do you wish to restart the server now? (y/n) [y]: y
Restarting Server ... OK
```

8. Check the Standby Operation Center's VPN tunnel server settings, which are used for communications between the Operations Center and its Collectors, before proceeding:

```
example-oc> show tunserver
CA configured: Yes
Server configured: Yes
ServerPublicName: 172.23.27.170
Proto: tcp
Port: 443
KeySize: 1024
Network: 5.0.0.0
Cipher: AES-128-CBC Compression: Yes
Service running: Yes
Reference Network Automation SN: N/A
Reference Network Automation Import: Skipped

Client Sessions:
UnitSerialNo: 1200201202100020
UnitName: oc-170-coll-1
UnitIPAddress: 5.0.0.15
Network: ExampleNet
UnitID: 1
Status: Offline: Last seen 2013-02-21 03:01:01
...
```

9. Using a Web browser, log in to the Standby Operations Center. Note that the admin password for the Standby Operations Center system will be set to the password of the Primary Operations Center.
10. In Settings -> Setup -> Collectors and Groups, re-enable all data collectors needed for the configuration.

Note: You must re-enable SNMP collection on this page, as it is automatically disabled on a restore.

11. In Settings –> Setup –> Network Automation Tunnels, verify that all Collectors are listed and appear as shown in the following figure (your list of Collectors will differ).
12. Register the above Collectors to the Standby Operations Center by executing the following commands on each of the Collectors. You use these commands to specify the Standby Operations Center IP address and new admin credentials:

```
admin-collector111.corp100.com> reset tunclient

admin-collector111.corp100.com> configure tunclient
```

13. Verify Operations Center Collector registration and communication by entering the following:

    ```
    example-oc> show tunclient
    Client configured: Yes
    Server: 172.23.27.182
    Proto: tcp
    Port: 443
    Cipher: AES-128-CBC
    Compression: On
    Tunnel Server IP: 5.0.0.1
    Tunnel Client IP: 5.0.0.10
    Server reachable: Yes Service
    running: Yes
    Latest Service Log Entries:
    Apr 10 17:02:51 localhost openvpn[20804]: VERIFY KU OK
    Apr 10 17:02:51 localhost openvpn[20804]: Validating certificate extended key usage
    Apr 10 17:02:51 localhost openvpn[20804]: ++ Certificate has EKU (str) TLS Web Server
    Authentication, expects TLS Web Server Authentication
    Apr 10 17:02:51 localhost openvpn[20804]: VERIFY EKU OK
    Apr 10 17:02:51 localhost openvpn[20804]: VERIFY OK: depth=0,
    /C=US/ST=CA/L=Santa_Clara/O=Infoblox/OU=na_Operations_Center/CN=OC182/name=Tunnel-S
    erver/emailAddress=support@infoblox.com
    Apr 10 17:02:51 localhost openvpn[20804]: Data Channel Encrypt: Cipher 'AES-128-CBC'
    initialized with 128 bit key
    Apr 10 17:02:51 localhost openvpn[20804]: Data Channel Encrypt: Using 160 bit message
    hash 'SHA1' for HMAC authentication
    Apr 10 17:02:51 localhost openvpn[20804]: Data Channel Decrypt: Cipher 'AES-128-CBC'
    initialized with 128 bit key
    Apr 10 17:02:51 localhost openvpn[20804]: Data Channel Decrypt: Using 160 bit message
    hash 'SHA1' for HMAC authentication
    Apr 10 17:02:51 localhost openvpn[20804]: Control Channel: TLSv1, cipher TLSv1/SSLv3
    DHE-RSA-AES256-SHA, 1024 bit RSA
    example-oc>
    ```

14. Log back in to the Standby Operations Center UI. In Settings –> Setup –> Network Automation Tunnels, verify that each of the registered Collectors are online. The Operations Center will begin receiving data from collectors immediately after connection is established. Data processing and analysis will catch up in a time interval similar to how long the collectors were offline.

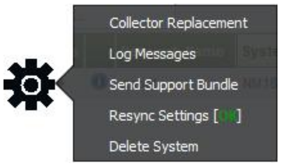
15. In Settings –> Database Settings –> Scheduled Archive, define the new archiving settings that you will need for the new Operations Center system, including enabling automatic archiving, defining the recurrence pattern.

Collector Replacement/Failover Procedure

Note: Database restoration is not needed or supported on Collectors. Collectors contain a very limited set of at any given time. The data that can be restored is pushed form the Operations Center to the collector at the time they register. After executing the `configure tunclient` command noted below, the Operations Center automatically pushes all previous Collector settings to the replacement Collector and the Collector begins its normal Discovery tasks.

To replace a Collector in an Operations Center environment, complete the following:

1. On the Operations Center, go to Settings –> Setup –> Network Automation Tunnels.
2. Click the Action icon in the row for the Collector you want to replace and choose Collector Replacement.



3. Change the serial number of the existing Collector to that of the replacement Collector.
4. Click OK.
5. On the replacement Collector, open a new Admin Shell session using SSH and complete the configuration commands for a basic setup.

   — Install the license for the replacement Collector:

   ```
   admin-na240.corp100.com> license <license filename>.gpg
   ```

   — Define server settings for the replacement Collector:

   ```
   admin-na240.corp100.com> configure server
   ```

   — Register the replacement Collector to the Operations Center IP Address, and define the Operations Center Network to which the Collector belongs.

   ```
   admin-na240.corp100.com> configure tunclient
   ```

   After executing the `configure tunclient` command, the Operations Center automatically pushes all previous Collector settings to the replacement Collector.

6. Log in to the Operations Center and verify that the replacement Collector status is Connected (Settings –> Setup –> Network Automation Tunnels, check Status column).
7. You can use SSH to log in the Operation Center's Admin Shell, to view a listing of the OC system and the Collectors. The `show tunserver` command shows each Collector's status in its listing.