

# BroadWorks Servers R25 Upgrade Method Of Procedure

## Contents

[Introduction](#)

[Standard Procedures](#)

[Installation Procedure](#)

[Network Function Manager \(NFM\)](#)

[Database Server \(DBS\)](#)

[Network Database Server \(NDS\)](#)

[Network Server \(NS\)](#)

[Media Server \(MS\)](#)

[Application Server \(AS\)](#)

[Service Control Function \(SCF\)](#)

[Application Delivery Platform \(ADP\)](#)

## Introduction

This document describes the generic upgrade Method Of Procedure (MOP) for upgrading BroadWorks servers as compiled by the BroadWorks Upgrade Team from other official documentation sources.

These reference documents are found on the [Cisco BroadWorks Documentation Guide Release 25](#) page. Refer to these main documents:

- [Software Management Guide](#)
- [System Configuration Guide](#)
- [Maintenance Guide](#)
- [Release 25.0 Release Notes](#)
- [AS Release 24.0 Release Notes](#)

For additional upgrade support reach out to the Upgrade Team at [bwupgrade@cisco.com](mailto:bwupgrade@cisco.com).

## Release Notes

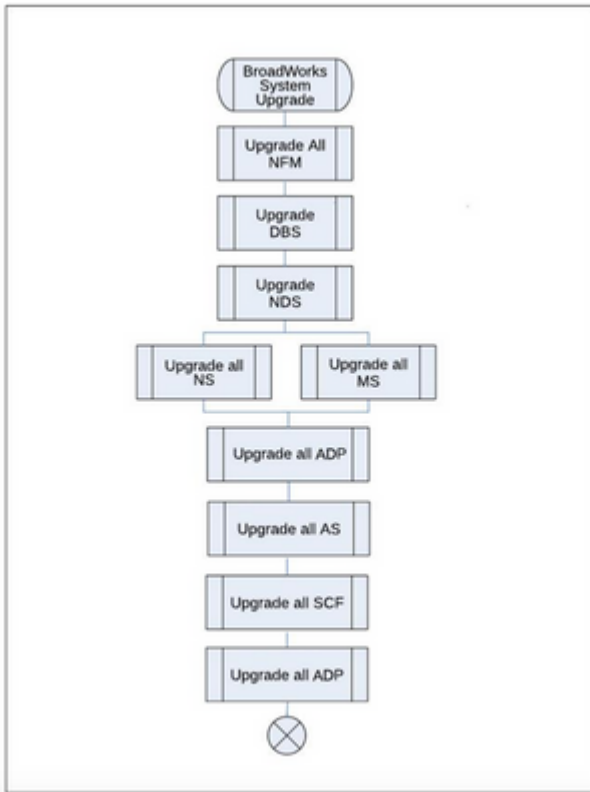
Prior to upgrade, review the release notes for the target release found in [Cisco BroadWorks Documentation Guide Release 25](#). Measure the potential impact with the changes noted.

If upgrading to a release more than one major number higher than the current release, (for example, upgrading from R23 to R25) review the release notes of the release(s) in between (R24 in this example).

These can be found on Cisco Documentation page or via the provided links.

## Standard Procedures

This is the order that servers are to be upgraded. The Network Servers (NSs) and Media Servers (MSs) do not need to be upgraded in a specific order in relation to each other.



The Application Delivery Platforms (ADPs) are mentioned twice in the sequence, as the first set of ADPs consist of the ones running DBSObserver, DBManagement and other Profile services. The second set of ADPs consist of the Xtended Services Interface (XSI), Open Client Interface - Provisioning (OCI-P), Device Management System (DMS), and Notification Push Server (NPS) services.

When upgrading any BroadWorks servers, follow these standard high-level steps:

1. Back up the server.
2. Install the latest Release Independent (RI) installation software package. The swmanager is included in the RI package.
3. Install the target release license.
4. Run the upgrade check tool from the CLI to ensure there are no warnings:

```
<#root>
```

```
ADP_CLI/Maintenance/Tools>
```

```
upgradeCheck ADP_Re1_2021.02_1.50
```

Always install the target release on **all peers of the same cluster** before upgrading one of the clusterâ€™s members.

It might be useful to check off completed tasks for each server. For example:

Machine	SERVER1	SERVER2	SERVER3
<b>Backup</b>	Done	Done	

<b>Tech Support</b>	Done	â€¦etcâ€¦	
<b>Target Release Install</b>	Done		
<b>License Import</b>	Done		
<b>Healthmon Check</b>	Done		
<b>Upgrade Check</b>	Done		

## Procedure Expectations

This document assumes that:

1. There is sufficient disk space to perform backups, install the new binaries, and upgrade.
2. Each server has the ability to install packages.
3. The OS is compatible with the target release.
4. The pre-InstallCheck has been run on every server and any warnings or failures have been corrected.
5. The system is in a health state.
6. Proper licenses have been obtained.
7. A post-upgrade test plan has been created, run prior to the upgrade, and the results recorded.

## Server Specific Notes

- The Network Function Manager (NFM) is independent of the other BroadWorks servers, so interoperability is not an issue. It is always recommended to run the latest version of the NFM.
- The upgrade to the Database Server (DBS) upgrades the software, but the schema changes to the database do not take place until the ADP (running the EnhancedCallLogsDBManagement application) is upgraded.
- It is recommended to back up the DBS or Network Database Server (NDS) before upgrading any ADP running EnhancedCallLogsDBManagementNDS or CCReportingDBManagement.
- Upgrade the MS/NS before the Application Server (AS). It is typical to leave the MS/NS running on the latest release for a day or two until the AS is upgraded.

Refer to the [Compatibility Matrix](#) for details.

## Pre-Upgrade and Post-Upgrade Test Plans

It is recommended to have a complete test plan, and to run and record the results of this test plan before an upgrade. This helps identify issues prior to an upgrade in addition to providing a comparison to post-upgrade test results.

## Reverts and Rollbacks

In the context of a BroadWorks upgrade, reverting and rolling back a server are not the same thing. A server revert restores the last database (DB) backup taken to restore the DB back to its state prior to the upgrade. With a revert any data added to the DB after the initial upgrade is lost. A rollback backs out all the changes

made to the DB in the process of the upgrade leaving any data added to the DB after the initial upgrade intact.

## Release Independent Servers

All servers are RI. All new features, bugs, and security fixes are delivered in a new version of the software. Patches will not be made available. Servers need to be upgraded from one version to another in order to obtain a fix. It is expected that a new version of each server will be released per month (instead of monthly patch bundles).

RI versions follow a different format than the standard Rel\_25.0\_1.944 format. This RI format is as follows, Server\_Rel\_YYYY.mm\_1.xxx:

- Server is MS, for example
- yyyy is the 4 digit year
- mm is the 2 digit month
- xxx is the incremental release for that month

For example, MS\_Rel\_2022.11\_1.273.Linux-x86\_64.bin is a version of the MS released in November of 2022.

## ADP

In Release 25, the Xtended Services Platform (XSP) and Profile Server (PS) functional offering has transitioned to the ADP. The applications that run on the XSP and PS are in two categories, core applications (providing services to the core infrastructure) or border applications (providing external API access). The applications that are installed define where the ADP lies in the network.

The applications delivered on the ADP are delivered either in RI fashion or delivered as Release Anchored (RA). RA means the application has a schema dependency on the AS version so there is a release component to the application filename and a different "branch" is delivered which is associated with the AS release.

See [BroadWorks Application Delivery Platform Software Download](#) for a list of the available applications for the ADP and the latest versions available.

## Installation Procedure

BroadWorks installers can be downloaded from [Cisco BroadWorks - Downloads](#).

### Install the Target Release Binary

Installing these can be done without service interruption. The install procedure is the same for all servers with one slight difference for server types. RI servers do not have an installation patch.

In these example steps, we are using an AS but the procedure is the same for all 25.x BroadWorks binaries. This must be performed as the root user (sudo is not acceptable.). The umask is 0022 for root and 0002 for bwadmin.

```
<#root>
```

```
$
```

```
chmod +x AS-25_Rel_2023.03_1.411.Linux-x86_64.bin
```

```
$
```

```
./AS-25_Rel_2023.03_1.411.Linux-x86_64.bin
```

Once the installation is complete, check the output for any additional actions or warnings. It displays messages that a new license is required and that the target release must be manually activated.

```
=====  
                The installation is now completed.  
=====
```

```
+++ Warnings summary +++  
+++WARNING --- 1001 <You may have to install new license files>  
+++WARNING --- 1002 <You will need to manually activate the new software version>
```

Please refer to the information reported in file:  
/var/broadworks/logs/installation/installation.230418.20h03m19s.warning  
for details as some warnings may require manual intervention.

```
done  
Moving logs, steps and warnings to /var/broadworks/logs/installation
```

Once installed, enter the `qversions` command from the `bwcli` in order to ensure it is present. Note that the status is **Installed** (not **Active**).

```
<#root>  
  
AS_CLI>  
  
qversions
```

Identity	Version	Install Date	Status
AS	2023.03_1.411	Apr 18, 2023	Installed
AS	24.0_1.944	Feb 11, 2022	Active

## Remove an Installed Binary

If the binary does not install correctly or needs to be removed, run the `uninstall-bwserver.pl` script.

```
<#root>  
  
$  
  
cd /bw/broadworks/<server>/uninstall/  
  
$  
  
./uninstall-bwserver.pl -r
```

The `-r` parameter gives the instruction to remove the remaining folder structure in `/bw/broadworks/<server>`.

## Install Target Release License

This section covers Universal Unique Identifier (UUID) licenses only, for NFM based licenses refer to the License Management section of the [Network Function Manager Node and License Management Guide](#).

For UUID based licenses the license files might be within multiple zip files, the server expects the zip file containing the .txt and .sig files. Do not unzip the files on a local machine to simply copy the .txt and .sig files as this invalidates the signature.

## Import License From the CLI

No need to unzip the licenses files and use the full path.

```
<#root>  
AS_CLI/System/Licensing/LicenseManager/LicenseStore>  
import /path/to/licensefiles.zip
```

## Install License From the OS

No need to unzip the licenses files and use the full path, as bwadmin or root run.

```
<#root>  
$  
cd /usr/local/broadworks/bw_base/bin/  
$  
./install-license.pl /path/to/licensefiles.zip
```

## Run the UpgradeCheck Tool

Run the `upgradeCheck` tool from the `bwcli` and confirm there are no warnings.

An example from the AS is shown here:

```
<#root>  
AS_CLI/Maintenance/Tools>  
upgradeCheck AS_Re1_2023.03_1.411
```

This is a dry-run upgrade.

BroadWorks SW Manager checking AS server version 2023.03\_1.411...  
Checking license file information  
Checking configuration file presences  
Checking installation.conf file  
Checking version presences  
Checking Broadworks version dependencies  
Checking target Broadworks version present  
Checking for available disk space  
Space required = 32768 Mb  
[done]  
Checking System configuration  
BW Daemon configuration validation  
testing /etc/xinetd.d... [done]  
Validating MoDaemon  
Checking upgrade compatibility  
Checking for dangling softlink  
...Monitoring directory tree starting at: /var/broadworks  
Running /usr/local/broadworks/AS\_Rel\_2023.03\_1.411 /bin/preUpgradeCheck  
Executing transform... [ok]

##### CCRS Support Check START #####

No need to check for CCRS devices, upgrading from release 19 or later

##### CCRS Support Check END #####

##### Conference Access Check START #####

No need to check for duplicate conference Id's and Moderator Pins , upgrading from release 19 or later

##### Conference Access Check END #####

##### trunk group check START #####

##### Startup Parameters IP Addresses Check START #####

##### Startup Parameters IP Addresses Check END #####

##### Reporting File Queues Check START #####

##### Reporting File Queues Check END #####

##### Domains table sanity check START #####

##### Domains table sanity check END #####

##### DNIS UID sanity check START #####

##### DNIS UID sanity check END #####

##### File System Protocol Check START #####

No need to check for use of WebDav interface for custom media files.  
Upgrading from release 20 or later

##### File System Protocol Check END #####

##### Disk space check for Announcement repository START #####

No need to check for available disk space for announcement repository.

Upgrading from release 20 or later

##### Disk space check for Announcement repository END #####

##### DeviceProfileAuthMode Check START #####

##### DeviceProfileAuthMode Check END #####

##### Activatable Feature Validation START #####  
Validation Successful

##### Activatable Feature Validation END #####

##### Database Manual Connections START #####  
No manual database connections detected..

##### Database Manual Connections END #####  
Waiting for maintenance tasks to complete if any  
Checking sshd configuration  
Checking for critical patches  
Checking for feature patches conformity between source and target version  
Checking TimesTen permanent memory size  
Checking version of active TimesTen

##### Database Impacts Check START #####

Database impacts detected: datastore will be unloaded, replication will be restarted, database will  
##### Database Impacts Check END #####  
setactiveserver command successfully executed.

Dry-run upgrade completed.

## Network Function Manager (NFM)

The NFM implements the Network and License Management functions.

Ensure healthmon shows no issues:

```
-----  
System Health Report Page  
BroadWorks Server Name: nfm1  
Date and time       : Thu Nov  8 05:19:16 EST 2022  
Report severity     : NOTIFICATION  
Server type         : NetworkFunctionManager  
Server state        : Unlock  
-----
```

No abnormal condition detected.

## Backup and Tech-Support



Prior to any server upgrade, it is recommended to take a backup and log a tech-support from prior to upgrade:

```
<#root>
$
bwBackup.pl -full -file=/var/broadworks/backup/bwBackup.bak
$
tech-support
>> tsup_hostname_sourceRelease.txt
```

## Pre-Upgrade

Run the upgradeCheck tool in order to ensure no warnings are issued:

```
<#root>
NFM_CLI/Maintenance/Tools>
upgradeCheck NFM_Rel_2022.11_1.274
```

## Verify if NetworkMonitoring is Present on the NFM Being Upgraded

```
<#root>
NFM_CLI/Applications/NetworkMonitoring/Replication>
status

Admin state = standby
Effective state = standby

      Name  Admin State  Effective State
=====
      PostgreSQL      Online      Online
      OpenNMS         Offline     Offline
      File replication  Online     Offline
      Monitoring      Online     Offline

4 entries found.

NFM_CLI/Applications/NetworkMonitoring/Replication>
exit

Please confirm (Yes, Y, No, N):

y

This session is now ending...
bwadmin@nfm02-cormac.local$ pgctl status
```

Database Status: Running  
Accepting Connections: TRUE  
Configured Mode: standby  
Effective Mode: standby  
Replication stats:  
WAL files: 66

## NFM Upgrade Switch

In a cluster, the order in which NFM servers are upgraded is not relevant. However, upgrade them one at a time.

Start the upgrade by entering this command:

```
<#root>
```

```
NFM_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server NFM 2022.11_1.274
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of NFM to 2022.11_1.274. NOTE that this action will  
Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

## License Management on the NFM

See the NFM [Node and License Management Guide](#).

## NFM Post-Upgrade Checks

Post upgrade, check the NFM status after startup:

- `healthmon -l`
- `showrun`
- `bwshowver`
- `mdbctl status`
- If Network Monitoring is active: `pgctl status`
- Review `/var/broadworks/logs/maintenance/ setactiveserver.NFM.Rel_2022.11_1.274.<date-time>.log` file for any potential activation errors.
- If the NFM is running NetworkMonitoring, ensure the application has come back up in the target release.

## Recommended NFM Post-Upgrade Tests

Verify that applications connected to the NFM servers are able to do database transactions.

These tests are generic, run any additional tests in the post-upgrade test plan.

## NFM Server Revert

The NFM revert procedure is the same as other servers.

The NFM revert to R21.SP1 is not supported as database encryption is not supported in that release. We must use the revert option there. Reverting an NFM cluster creates downtime for applications since the database must be stopped on all cluster members to restore the database backup.

The detailed revert steps can be found in the [NFM Configuration Guide](#).

### Revert

In the event that the NFM does not pass the post upgrade checks, revert to the previous release.

```
<#root>
```

```
NFM_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server NFM 2022.10_1.318 revert
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of NFM to 2022.10_1.318 NOTE that this action will  
Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

In the example, it is reverting back to 2022.10\_1.318 but this can be substituted for any previous release.

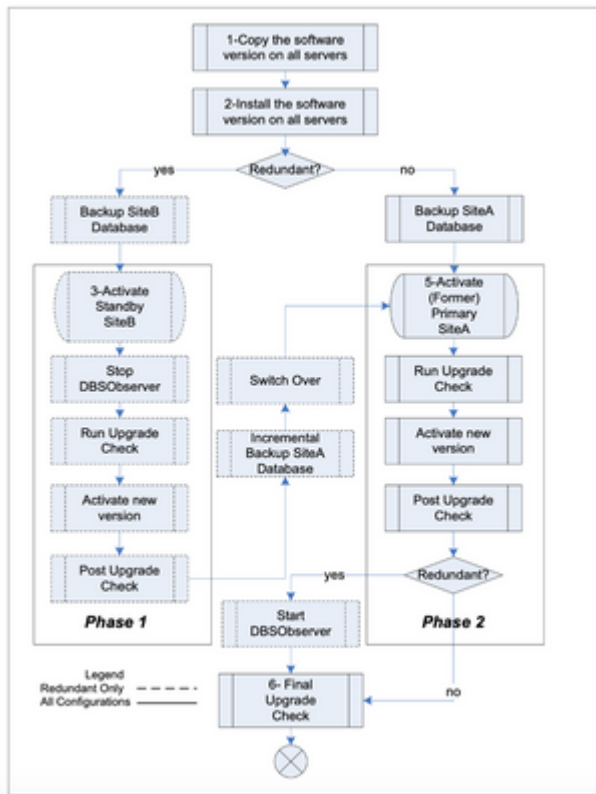
## Database Server (DBS)

Since the DBS runs a different database engine (Oracle 11g) than other BroadWorks products, the upgrade prerequisites and upgrade steps and backup commands are quite different than the rest of the BroadWorks suite. Make sure to read this section thoroughly, and do not hesitate to raise informational tickets to the Technical Assistance Center (TAC) in order to get any clarifications needed.

One difference that stands out, for the DBS, and the DBS only, start upgrading the Standby server first. This is done as the DBS upgrade does not actually change the DB schema. This happens when CCReportingDBManagement is **upgraded**. With a DBS upgrade, the software and database are upgraded *but the schema does not change*.

Other particularities include the need to reboot the servers before running an upgrade, as well as manually removing scheduled tasks (so to not interfere with the upgrade).

Everything needed is thoroughly described in the next sections. The upgrade sequence diagram is followed by the detailed steps and commands for each step.



## Backup Both DBS

Note the size of the DATA with the `dbsetl diskinfo` command.

```
<#root>
```

```
bwadmin@dbs1$
```

```
dbsetl diskinfo
```

```
Disk Group Usage Summary
```

```
DATA 12.32 % used (8075/65530 MB)
FRA 11.12 % used (7286/65530 MB)
FRA LIM 11.50 % used (7156/62253 MB)
FRA 11.12 % used (7286/65530 MB) , w/o Reclaimable data
```

```
Disk Usage Summary
```

```
DATA 12.32 % used (8075/65530 MB)
FRA 11.12 % used (7286/65530 MB)
```

```
Rebalancing in progress: no
```

The required space for the backup is approximately 1/7<sup>th</sup> of that.

Enter these commands to back up:

```
<#root>
```

```
bwadmin@dbs1$
```

```
export TAG=`echo -n $(showver | grep Rel | sed -e 's|.*Rel_||' | tr -d '\n'); echo -n ' -â€œ-â€œ; date +%Y.%m.%d`
```

```
bwadmin@dbs1$
```

```
bwBackup.pl -type=Full -tag=$TAG -path= /var/broadworks/backup/$TAG -compressed
```

```
BroadWorks Database Server Backup Tool version 1.10
```

```
Checking for sufficient disk spaceâ€¦ [DONE]
```

```
Backing up database... [DONE]
```

```
bwadmin@dbs1$
```

Note the backup is run as the Oracle user so it needs to be written to somewhere that Oracle has write permissions to. Ensure that there is sufficient disk space to handle this on the partition.

Full backups can be run using: this command:

```
<#root>
```

```
bwadmin@dbs1$
```

```
bwBackup.pl -f -type=full -tag=$TAG -device=/var/broadworks/backup/$TAG
```

## Stop DBSObserver

For redundant configurations, stop the DBSObserver application on the ADP while upgrading:

```
<#root>
```

```
bwadmin@<ps1>$
```

```
stopbw DBSObserver
```

The DBSObserver is deployed on one of the ADPs. In order to determine if a given ADP is running the DBSObserver, look at the output of the `showrun` command on the ADP.

## Pre-Upgrade Sanity Checks

Ensure replication is running and healthy and that the DBs are correctly in place with the `dbctl status` command on both DBSs.

```
<#root>
```

```
bwadmin@dbs1$
```

```
dbctl status
```

```
Database Name           : bwCentralizedDb0
Database Instance       : DBSI0
Database Service        : bwCentralizedDb
Database Status (Mode)  : running (Read Write)
```

Database Service Status : running  
Database Role (Expected Role) : Primary (Primary)

bwadmin@dbs2\$

**dbstl status**

Database Name : bwCentralizedDb1  
Database Instance : DBSI0  
Database Service : bwCentralizedDb  
Database Status (Mode) : running (Read Only w/Apply)  
Database Service Status : running  
Database Role (Expected Role) : Secondary (Secondary)  
Check repctl status to ensure that logs are shipping and both DBS are in sync.

bwadmin@dbs1\$

**repctl status**

Gathering site information, please be patient... [DONE]  
Redundancy/Replication Status

-----  
Database Name = bwCentralizedDb1  
Database Service Name = bwCentralizedDb  
Dataguard Replication pid = 26502  
Primary Database = bwCentralizedDb0 [DBS1]  
Standby Database = bwCentralizedDb1 [DBS2]  
Primary Database Reachable = yes  
Standby Database Reachable = yes  
Replication gap summary = OK  
Replication gap details  
    Primary SCN: 842675099  
    Standby SCN: 842675095  
Redo Apply Lag = +00 00:00:00  
Estimated Redo Rate = 0.01 MB/s  
Primary Estimated Redo Log Space = 791991 MB  
Primary Estimated Log Space Exhaustion = +916 15:45:00  
Primary Redo free space condition = NORMAL  
Primary Lag vs Redo state = N/A  
Standby Estimated Redo Log Space = 788521 MB  
Standby Estimated Log Space Exhaustion = +912 15:21:40  
Standby Redo free space condition = NORMAL  
Standby Lag vs Redo state = N/A  
Archive gap summary = N/A  
Archive gap details N/A

## Pre-Upgrade Mandatory Steps

### Remove the Scheduled tasks from the Scheduler

Scheduled tasks have been identified to cause upgrade failure and auto-revert to source release. First take note of the initial configuration:

<#root>

```
DBS_CLI/Maintenance/Scheduler>
```

```
get
```

Id	Name	Date	Day	Hour	Minute
1	tech-support	-	-	4	33
2	cpuMon	-	-	-	5
3	healthmon	-	-	-	30(offset: 1)
4	autoCleanup	-	saturday	2	33
5	backup	-	saturday	4	03

Then remove the scheduled tasks. Watch out when removing a task, the Id numbers shift. Start by removing the highest Id first.

```
<#root>
```

```
DBS_CLI/Maintenance/Scheduler>
```

```
del 5
```

```
DBS_CLI/Maintenance/Scheduler>
```

```
del 4
```

```
DBS_CLI/Maintenance/Scheduler>
```

```
del 3
```

```
DBS_CLI/Maintenance/Scheduler>
```

```
del 2
```

```
DBS_CLI/Maintenance/Scheduler>
```

```
del 1
```

Verify the entries have been deleted with the `get` command.

## Reboot the Server (init 6) Before Upgrading

Make sure to reboot each server before upgrading. Again, this helps avoid upgrade failure. Since we are always doing the upgrade on a standby DBS server, it does not affect anything and does not cause more roles switching than normally.

**Refer to the upgrade sequence diagram for the order. The init 6 is executed after the backup and before the activation of each server.**

## Launch the Upgrade

The DBS differs from all other BroadWorks servers in that the standby/secondary DBS is upgraded first. If starting with the currently active server; it requires an extra reboot / role change.

On the Standby/Secondary:

```
<#root>
```

```
DBS_CLI/Maintenance/ManagedObjects>
```

```
lock
```

Switch to the target release:

```
<#root>
```

```
DBS_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server 2023.03_1.411
```

Once complete, unlock the server:

```
<#root>
```

```
DBS_CLI/Maintenance/ManagedObjects>
```

```
unlock
```

Check healthmon in order to ensure that the DBS has started up correctly.

## Switchover the Newly Upgraded STANDBY/Secondary DBS to be Active/Primary

---

**Note:** Run this command on the newly upgraded server (not the DBS still at the previous release).

---

```
<#root>
```

```
bwadmin@dbs1$
```

```
peerctl ls
```

PEER	Role	Status	State
===== dbs1	PRIMARY	ACTIVE	Unlocked
dbs2	SECONDARY	STANDBY	Unlocked

```
bwadmin@dbs1$
```

```
peerctl setPrimary dbs2
```

```
Setting 'dbs2' as new primary.
```

```
Switch over may take a few moments to complete, do you still want to proceed? (y/n) [y]?
```

```
y
```

```
Switching over to 'bwCentralizedDb1', this may take a few moments to complete.[DONE]  
Switch over completed.
```



bwadmin@dbs1\$

peerctl ls

PEER	Role	Status	State
=====	=====	=====	=====
dbs1	SECONDARY	STANDBY	Unlocked
dbs2	PRIMARY	ACTIVE	Unlocked

At this stage, the upgraded DBS (dbs2) is now primary.

### Database Server Post-Upgrade Checks

- Place a call to a Call Center and retrieve reports that show this activity.
- Retrieve historical reports.
- Review XSLogs on the AS in order to confirm the data is being shipped to DBS2 (and not in file queue).

### Upgrade the Former Primary (now Standby)

On the former Primary <dbs1> (now standby), lock:

<#root>

DBS\_CLI/Maintenance/ManagedObjects>

lock

Switch it to the destination release:

<#root>

DBS\_CLI/Maintenance/ManagedObjects>

set activeSoftwareVersion server DBS 2023.03\_1.411

Unlock the primary dbs1:

<#root>

DBS\_CLI/Maintenance/ManagedObjects>

unlock

### Perform the Switchover to be the Original Setup the Standby to be Primary

Set DBS1 back to primary with the peerctl setPrimary dbs1 command.

```
<#root>
```

```
bwadmin@dbs1$
```

```
peerctl ls
```

PEER	Role	Status	State
=====	=====	=====	=====
dbs1	SECONDARY	STANDBY	Unlocked
dbs2	PRIMARY	ACTIVE	Unlocked

```
bwadmin@dbs1$
```

```
peerctl setPrimary dbs1
```

```
Setting 'dbs1' as new primary.
```

```
Switch over may take a few moments to complete, do you still want to proceed? (y/n) [y]?
```

```
y
```

```
Switching over to 'bwCentralizedDb0', this may take a few moments to complete.[DONE]  
Switch over completed.
```

```
bwadmin@dbs1$
```

```
peerctl ls
```

PEER	Role	Status	State
=====	=====	=====	=====
dbs1	PRIMARY	ACTIVE	Unlocked
dbs2	SECONDARY	STANDBY	Unlocked

## Reset the Scheduler Back as it was Before

Since we removed the scheduled tasks from the scheduler we need to add those again. Just in case, here are all the standard timings:

```
<#root>
```

```
DBS_CLI/Maintenance/Scheduler>
```

```
add tech-support daily 4 33
```

```
DBS_CLI/Maintenance/Scheduler>
```

```
add cpuMon minute 5
```

```
DBS_CLI/Maintenance/Scheduler>
```

```
add healthmon minute 30 1
```

```
DBS_CLI/Maintenance/Scheduler>
```

```
add autoCleanup day saturday 2 33
```

```
DBS_CLI/Maintenance/Scheduler>
```

```
add backup day saturday 4 3
```

## Primary Database Server Post-Upgrade Checks

- Place a call to a Call Center and retrieve reports that show this activity.
- Retrieve historical reports.
- Review XSLogs on the AS in order to confirm the data is being shipped to DBS1 (and not in file queue).

Check healthmon, replication and redo log shipping:

```
<#root>
bwadmin@dbs1$
repctl status
bwadmin@dbs1$
dbsctl status
bwadmin@dbs1$
dbsctl diskinfo
bwadmin@dbs1$
dbsctl redolog info
```

Perform this on both DBSs in order to confirm they are in good health post upgrade.

## Validate Health from the ADP

From the ADP running CCReportingDBManagement, enter these commands:

```
<#root>
bwadmin@ps1$
bwcli
ADP_CLI/Applications/CCReportingDBManagement/Database/Databases/Sites>
validate
Host Name Database Status
=====
dbs01 bwCentralizedDb Primary
dbs02 bwCentralizedDb Standby
ADP_CLI/Applications/CCReportingDBManagement/Database/Schemas> validate
Name Status
=====bweccr Read/Write
```

## Start DBSObserver

Once both DBSs are upgraded, start the DBSObserver application to control failover:

```
<#root>
```

```
bwadmin@ADP1$
```

```
startbw DBSObserver
```

```
Starting DBSObserver...
```

## Database Server Revert Procedure

The overall Database Server revert procedure is very similar to the general BroadWorks revert procedure described in the *BroadWorks Software Management Guide*.

The main differences are as follows:

- Rollback is not supported. Only revert is supported.
- For redundant configurations, the software revert is done on the standby site first.
- A post revertcheck (see [Database Server > Database Server Revert Procedure > Detailed Procedural Steps > Post Revertcheck](#)) must be executed after software activation to verify if the revert of the database was done properly and if any corrective action is necessary.

## Rollback Denied

Any attempt to roll back the active software version on the Database Server is denied, as shown in this example:

```
<#root>
```

```
DBS_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server DBS 2022.12_1.371
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of DBS to 2022.12_1.371. NOTE that this action will  
Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

```
SW Manager initialized!
```

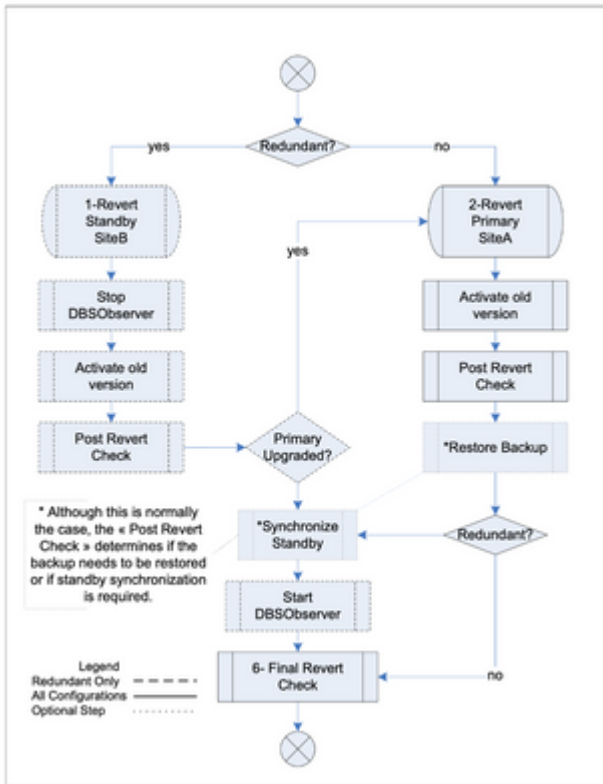
```
[Error] This server type does not support rollback. The revert flag is mandatory.
```

## Detailed Procedural Steps

The steps required to revert Cisco BroadWorks on a standalone server and on a redundant server configuration are identical and must be done in a specific order. These steps cover both configurations.

1. Activate the old Cisco BroadWorks version. For redundant configurations, the standby server must be reverted first. When reverting the standby, do not specify a backup location.
2. For redundant configurations, proceed with the reversal of the primary server.
3. Perform the post revert verification.

In order to add clarity to the steps corresponding to the sequence diagram, when we revert standby SiteB we do not specify the backup file. But we can specify the backup file when we revert SiteA. Alternatively, we can restore the backup file in the next step. The synchronize standby step then syncs the data between SiteA and SiteB.



## Revert Operation

The revert operation is initiated from the BroadWorks *CLI ManagedObject* level. As with the other server types, the backup location can be specified directly within the CLI, as shown in this example:

```
<#root>
```

```
DBS_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server DBS 2022.12_1.371 revert /var/broadworks/backup/2022.12_1.371-2022.12.2
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of DBS to 2022.12_1.371. NOTE that this action will  
Continue?
```

However, when the revert operation is performed on the standby site, do not specify the backup location. The standby site is recreated from the primary using `importdb.pl` after the revert operation or automatically resynchronized by the revert script itself. Once the revert has been completed, see the `revertcheck` test results for the recommended corrective actions.

Furthermore, if the revert is executed before upgrading the primary, the database running on the primary is still unaffected by the upgrade, and the standby can be safely reverted to the previous release without requiring a restore or resynchronization operation.

This command output log shows the revert sequence when started without specifying a backup directory:

<#root>

DBS\_CLI/Maintenance/ManagedObjects>

```
set activeSoftwareVersion server DBS 2022.12_1.371 revert
```

## Post Revertcheck

The post *revertcheck* script is designed to determine if the revert of the database was done properly and if any corrective action is necessary. It must be executed from the latest BroadWorks release *bin* directory, using the full path or the dot-slash (./) prefix:

<#root>

bwadmin@dbs01.example.com\$

```
cd /usr/local/broadworks/DBS_Rel_2022.12_1.371/bin/
```

bwadmin@dbs01.example.com\$

```
./dbsctl validate revertcheck
```

The last activation completed 0d 18h 23m 39s ago.

Running database post revert checks...

Oracle version already active.

Grid version already active.

... reverting init check	[success]
... reverting check permissions	[skipped]
... reverting check hardware	[skipped]
... reverting check peer time	[skipped]
... reverting check kernel	[skipped]
... reverting check inventory	[skipped]
... reverting check archive/og	[skipped]
... reverting check backup	[skipped]
... reverting check standby count	[skipped]
... reverting check remote versions	[skipped]
... reverting check patch level	[skipped]
... reverting check peer idle	[skipped]
... reverting check node id	[skipped]
... reverting check replication	[success]
... reverting check peer status	[success]
... reverting check peer name lookup	[skipped]
... reverting check traced event	[skipped]
... reverting check invalid objects	[skipped]
... reverting check active tasks	[skipped]
... reverting check supported data types	[skipped]
... reverting check dbcontrol	[skipped]
... reverting check database status	[skipped]

Post check...

[DONE]

No corrective action necessary

## Restore Backup

If a backup directory was specified with the *set activeSoftwareVersion server* command, the backup is automatically restored by the revert process.

Otherwise, the backup needs to be restored using this command:

```
<#root>
```

```
bwadmin@dbs01$
```

```
bwRestore.pl -recover -path=/var/broadworks/backup/<backup_name>
```

## Synchronize Standby

If the standby needs to be resynchronized with the database, the `importdb.pl` script is used.

This command is used to resynchronize the database on Site B if the primary on Site A has not been upgraded:

```
<#root>
```

```
bwadmin@dbs02$
```

```
importdb.pl --peer=dbs01
```

If Site A was upgraded and reverted, the standby database needs to be recreated from the primary site and redundancy must be reconfigured. To do this, this command is used instead:

```
<#root>
```

```
bwadmin@dbs02$
```

```
importdb.pl --peer=dbs01 --cleanup
```

The revert procedure for the DBS is detailed further in the [DBS Configuration Guide](#).

## Switch Primary/Standby Back to Pre-Upgrade State

Once the revert is complete, use the `peerctl` command to set the servers back to the preupgrade Primary/Standby state. For example:

```
<#root>
```

```
bwadmin@dbs1$
```

```
peerctl setPrimary dbs1
```

If the DBSObserver is not running on the ADP, start it.

## Network Database Server (NDS)

Ensure healthmon shows no issues:

-----  
System Health Report Page

BroadWorks Server Name: nds1  
Date and time : Thu Nov 7 05:19:16 EST 2022  
Report severity : NOTIFICATION  
Server type : NDS  
Server state : Unlock  
-----

No abnormal condition detected.  
-----

## Backup and Tech-Support

Prior to any server upgrade, it is recommended to take a full backup and log a tech-support from prior to upgrade:

```
<#root>
```

```
$
```

```
bwBackup.pl -full -file=/var/broadworks/backup/bwBackup.bak
```

```
$
```

```
tech-support
```

```
>> tsup_hostname_sourceRelease.txt
```

## Upgrade Check

Run the upgradeCheck tool in order to ensure no warnings are issued:

```
<#root>
```

```
NDS_CLI/Maintenance/Tools>
```

```
upgradeCheck NDS_Re1_2022.11_1.273
```

## NDS Upgrade Switch

In a cluster, the order in which NDSs are upgraded is not relevant. However, only upgrade one at a time. Start the upgrade by entering this command:

```
<#root>
```

```
NDS_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server NDS 2022.11_1.273
```



+++ WARNING +++ WARNING +++ WARNING +++

This command will change the active software version of NDS to 2022.11\_1.273. NOTE that this action will  
Continue?

Please confirm (Yes, Y, No, N):

y

## NDS Post-Upgrade Checks

Post upgrade, check the NDS status after startup:

- `healthmon -l`
- `showrun`
- `bwshowver`
- `mdbctl status`
- Review `/var/broadworks/logs/maintenance/ setactiveserver.NDS.Rel_2022.11_1.273.<date-time>.log` file for any potential activation errors.

## Recommended NDS Post-Upgrade Tests

Verify that applications connected to the NDS are able to do database transactions.

These tests are generic, run any additional tests in the post-upgrade test plan.

## NDS Server Revert

Reverting back an NDS cluster creates downtime for applications since the database must be stopped on all cluster members in order to restore the database backup.

The NDS revert procedure is the same as other servers.

## Revert

In the event that the NDS does not pass the post upgrade checks, revert back to the previous release:

```
<#root>
```

```
NDS_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server NDS 2022.08_1.352 revert
```

+++ WARNING +++ WARNING +++ WARNING +++

This command will change the active software version of NDS to 2022.08\_1.352 NOTE that this action will  
Continue?

Please confirm (Yes, Y, No, N):

y

In the example, it is reverting back to 2022.08\_1.352 but this can be substituted for any previous release.

## Network Server (NS)

Note that the NS is now RI.

Ensure healthmon shows no issues

-----  
System Health Report Page

BroadWorks Server Name: ns1

Date and time : Thu Oct 3 15:50:21 BST 2022

Report severity : NOTIFICATION

Server type : NetworkServer

Server state : Unlock

-----  
No abnormal condition detected.  
-----

## Backup and Tech-Support

Prior to any server upgrade, it is recommended to take a backup and log a tech-support file:

```
<#root>
$
bwBackup.pl networkserver NS_hostname_sourceRelease.tar
$
tech-support
>> tsup_hostname_sourceRelease.txt
```

## Pre-Upgrade

Make a test call that invokes the NS and verify a successful 302 message is in the NSXSLog log located in /var/broadworks/logs/routingserver/.

Run the upgradeCheck tool in order to ensure no warnings are issued:

```
<#root>
NS_CLI/Maintenance/Tools>
upgradeCheck NS_Rel_2022.11.1.27
```

Check the current number of calls etc in use with the **qcurrent** command:

```
<#root>
```

```
NS_CLI/Monitoring/Report>
```

```
qcurrent
```

Check database sync (`synchcheck_basic.pl -a`) on all non-primary peer NSs:

```
<#root>
```

```
$
```

```
synchcheck_basic.pl -a
```

## Primary NS Upgrade Switch

Start the upgrade by entering this command:

```
<#root>
```

```
NS_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server NS 2022.11_1.27
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of NS to 2022.11_1.27. NOTE that this action will c  
Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

Update the database statistics by running the `bwPeriodMaint.sh` script.

```
<#root>
```

```
$
```

```
bwPeriodMaint.sh
```

## NS Post-Upgrade Checks

Post upgrade, check the NS status after startup.

- **healthmon -l**
  - It shows the peer is out of sync but this is expected until the secondary is upgraded.
  - If healthmon indicates that some database page sizes are surpassed, enter `check_dbpages.pl networkserver modify`.
- **showrun**
- **bwshowver**

- Review /var/broadworks/logs/maintenance/ setactiveserver.NS.Rel\_2022.11\_1.27.<date-time>.log file for any potential activation errors.
- Run NS tests to ensure that this NS is processing calls properly.

## Recommended NS Post-Upgrade Tests

- Validate Public Switched Telephone Network (PSTN) inbound 302 redirect.
- Validate AS outbound 302 redirect.
- Validate AS to MS request/response.
- Validate CLI access (log in and go to NS\_CLI/System/Device/HostingNE; enter the get command).
- Validate web access to the NS (if enabled).
- Validate user lookup from an ADP using NS mode communication by simply logging in to an ADP.

## NS Post-Upgrade Activities

Verify that the NS is not set to deny ADPs from logging into an AS at a different version. Set ADP Version Equal to false for each hostingNE under NS\_CLI/System/Device/HostingNE>.

## NS Revert

In the event that the NS does not pass the post upgrade checks, revert back to the previous release:

```
<#root>
```

```
NS_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server NS 2022.09_1.340 revert
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of NS to 2022.09_1.340. NOTE that this action will Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

In the example, it is reverting back to 2022.09\_1.340 but this can be substituted for any previous release.

As the secondary NS has a current version of the database from the source release, the DB can be imported from there.

On the secondary NS,

```
<#root>
```

```
$
```

```
repctl start
```

On the primary NS,

```
<#root>
```

```
$
```

```
stopbw
```

```
$
```

```
repctl stop
```

```
$
```

```
importdb.pl networkserver <peer_ns2>
```

```
$
```

```
repctl start
```

```
$
```

```
startbw
```

Unlock the secondary (and all other) NS databases:

```
<#root>
```

```
$
```

```
peerctl unlock
```

Verify that replication is running on the reverted primary NS:

```
<#root>
```

```
$
```

```
repctl status
```

Verify that replication is running on all secondary NSs and that the database is unlocked:

```
<#root>
```

```
$
```

```
repctl status
```

Check `healthmon -l` on all NSs. Ensure the reported severity is NOTIFICATION for all servers.

Verify that the secondary NS and primary NS databases are synchronized (on secondary):

```
<#root>
```

```
$
```

```
synchcheck_basic.pl -a
```

## Secondary NS Upgrade Switch

Start the upgrade by entering this command:

```
<#root>
```

```
NS_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server NS 2022.11_1.27
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of NS to 2022.11_1.27. NOTE that this action will c  
Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

No need to run the update statistics script, as it was run prior to the import that was automatically done during the upgrade of the secondary NS.

## NS Post-Upgrade Checks

Post upgrade, check the NS status after startup

- **healthmon -l**
  - If healthmon indicates that some database page sizes are surpassed, enter **check\_dbpages.pl networkserver modify**.
- **showrun**
- **bwshowver**
- Review `/var/broadworks/logs/maintenance/ setactiveserver.NS.Rel_2022.11_1.27.<date-time>.log` file for any potential activation errors.
- Run NS tests to ensure that this NS is processing calls properly.

## Recommended NS Post-Upgrade Tests

Locking the primary NS, this routes all traffic through the secondary:

- Validate PSTN inbound 302 redirect.
- Validate AS outbound 302 redirect.
- Validate AS to MS request/response.
- Validate CLI access (log in and go to `NS_CLI/System/Device/HostingNE`; enter the `get` command).
- Validate web access to the NS (if enabled).
- Validate user lookup from an XSP using NS mode communication by simply logging in to an XSP.
- Post-Cluster tests.
- Ensure healthmon reports severity NOTIFICATION for all servers.
- Check database synchronization.

```
<#root>
```

```
$
healthmon -l
$
synchcheck_basic.pl -a
```

## Media Server (MS)

Ensure healthmon shows no issues:

```
-----
System Health Report Page
BroadWorks Server Name: ms1
Date and time      : Thu Mar 3 11:10:53 BST 2022
Report severity   : NOTIFICATION
Server type       : MediaServer
Server state      : Unlock
-----
```

No abnormal condition detected.

## Backup and Tech-Support

Prior to any server upgrade, it is recommended to take a backup and log a tech-support from prior to upgrade. On the MS, this would be done with:

```
<#root>
$
bwAutoBackup.sh
$
tech-support
>> tsup_hostname_sourceRelease.txt
```

## Pre-Upgrade

Make a test call that invokes Interactive Voice Response (IVR) or retrieve a voicemail and ensure it works as expected and the call can be seen in the logs.

Run the upgradeCheck tool in order to ensure no warnings are issued:

<#root>

MS\_CLI/Maintenance/Tools>

```
upgradeCheck MS_Re1_2022.11_1.273
```

Check the current number of ports in use with the `qcurrent` command.

<#root>

MS\_CLI/Monitoring/Report>

```
qcurrent
```

## MS Upgrade Switch

Start the upgrade by issuing this command:

<#root>

MS\_CLI/Maintenance/ManagedObjects>

```
set activeSoftwareVersion server MS 2022.11_1.273
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of MS to 2022.11_1.273. NOTE that this action will  
Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

## MS Post-Upgrade Checks

Post upgrade, check the MS status after startup and verify leaving a voicemail and voicemail retrieval.

- `healthmon -l`
- `showrun`
- `bwshowver`

## Recommended MS Post-Upgrade Tests

- Validate successful voice mail deposit and retrieval.
- Validate successful IVR interaction.
- Validate successful Three-Way Call.

These tests are generic, run any additional tests in the post-upgrade test plan.

## MS Revert



In the event that the MS does not pass the post upgrade checks, revert back to the previous release.

```
MS_CLI/Maintenance/ManagedObjects> set activeSoftwareVersion server MS 2022.08_1.350 revert
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of MS to 2022.08_1.350. NOTE that this action will cause downtime.
```

```
Continue?
```

```
Please confirm (Yes, Y, No, N): y
```

In the previous example, it is reverting back to 2022.08\_1.350 but this can be substituted for any previous release.

## Application Server (AS)

Ensure healthmon shows no issues

```
-----  
System Health Report Page
```

```
BroadWorks Server Name: as1
```

```
Date and time      : Thu Oct 3 15:50:21 BST 2022
```

```
Report severity    : NOTIFICATION
```

```
Server type       : AppServer
```

```
Server state      : Unlock
```

```
-----  
No abnormal condition detected.
```

- ```
-----
```
- Check the logs to ensure that both ASs are processing calls (forcing new calls to the secondary can be done by locking AS1).
  - Validate web access through Web Servers and each AS.

## Backup and Tech-Support

It is recommended to take a backup and log a tech-support from prior to upgrade.

```
<#root>
```

```
$
```

```
bwBackup.pl AppServer AS_hostname_sourceRelease.tar
```

```
$
```

```
tech-support
```

```
>> tsup_hostname_sourceRelease.txt
```

## Pre-Upgrade

Run the upgradeCheck tool to ensure no warnings are issued.

```
<#root>
AS_CLI/Maintenance/Tools>
upgradeCheck AS_Rel_2023.03_1.411
```

---

**Note:** If the upgradeCheck fails because of files in the /var/broadworks/eccr or /var/broadworks/ecl directory, then wait until a "lock force" is performed from the bwcli. This purges the files to the DBS within a few minutes.

---

Check database sync (synchcheck\_basic.pl -a) on the secondary AS:

```
<#root>
$
synchcheck_basic.pl -a
```

Set the extensionTimeInSeconds to 10800 (three hours) to correspond with the amount of time reserved for upgrading the server:

```
<#root>
AS_CLI/System/Registration>
set extensionTimeInSeconds 10800
```

The typical setting for this is when not upgrading **2400** as per the [System Configuration Guide](#).

Replication pushes this change to the remaining servers in the cluster.

Delete the backup operation from the scheduler:

```
<#root>
AS_CLI/Maintenance/Scheduler>
get
```

| Id | Name   | Date | Day      | Hour | Minute |
|----|--------|------|----------|------|--------|
| 5  | backup | -    | saturday | 4    | 03     |

If the backup is triggered during the upgrade, it might cause issues during activation:

```
<#root>
```

```
AS_CLI/Maintenance/Scheduler>
```

```
del 5
```

## Lock the Primary AS

Lock the primary AS, new calls are through the secondary allowing the number of active calls on the primary to drop before performing the switch (switching or lock force causes the active calls to drop):

```
<#root>
```

```
AS_CLI/Maintenance/ManagedObjects>
```

```
lock
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will lock the server. Note that this action could cause downtime.
```

```
The server state is persisted across server restarts and upgrade.
```

```
A server in "Locked" state will need to be manually unlocked after a server restart or upgrade. Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

```
...Done
```

Once done, check the number of calls on the AS with the `qcurrent` command:

```
<#root>
```

```
AS_CLI/Monitoring/Report>
```

```
qcurrent
```

## Primary AS Upgrade Switch

Once the calls have dropped to an acceptable level, start the upgrade with:

```
<#root>
```

```
AS_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server AS 2023.03_1.411
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of AS to 2023.03_1.411 . NOTE that this action will  
Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

Once complete, unlock the server:

```
<#root>
```

```
AS_CLI/Maintenance/ManagedObjects>
```

```
unlock
```

Update the DB statistics with `bwPeriodMaint.sh`:

```
<#root>
```

```
$
```

```
bwPeriodMaint.sh
```

This command returns no output.

As we deleted the backup operation from the scheduler, we need to add it back post upgrade. This is the suggested value. We have to add it back to the value that was configured before the upgrade:

```
<#root>
```

```
AS_CLI/Maintenance/Scheduler>
```

```
add backup day saturday 4 3
```

## Primary AS Post-Upgrade Actions

### AS Post-Upgrade Checks

Post upgrade, check the AS status after startup and verify registrations and calls.

- `healthmon -l`
  - It shows the peer is out of sync but this is expected until the secondary is upgraded.
- `showrun`

- `bwshowver`
- Review `/var/broadworks/logs/maintenance/ setactiveserver.AS.Rel_2023.03_1.411 .<date-time>.log` file for any potential activation errors.
- Run AS tests to ensure that this AS is processing calls properly.

## Recommended AS Post-Upgrade Tests

- Validate SIP outbound calling.
- Validate Media Gateway Control Protocol (MGCP) outbound calling.
- Validate PSTN to SIP user inbound calling.
- Validate PSTN to MGCP user inbound calling.
- Validate voice mail leaving/retrieval (voice portal).
- Validate CommPilot originations/terminations.
- Validate CLI access (go to `AS_CLI/System/Alias` and use the `get` command).
- Validate direct web access to the AS.

## Localized Voice Prompts

If upgrading to R25, the custom audio prompts are copied automatically from the source release. Refer to Section 4.5 in the [Feature Description](#).

## AS Revert

In the event that the AS does not pass the post upgrade checks, revert back to the previous release.

```
<#root>
```

```
AS_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server AS 2022.08_1.354 revert
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of AS to 2022.08_1.354. NOTE that this action will Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

In the example, it is reverting back to `2022.08_1.354`, but this can be substituted for any previous release.

As the secondary AS has a current version of the database, import the DB from there.

On the secondary AS:

```
<#root>
```

```
$
```

```
repctl start
```

On the primary AS:

```
<#root>
$
stopbw
$
repctl stop
$
importdb.pl appserver <peer_as2> appserver
$
repctl start
$
startbw
```

Unlock the secondary AS database:

```
<#root>
$
peerctl unlock
```

Verify that replication is running on the reverted primary AS:

```
<#root>
$
repctl status
```

Verify that replication is running on the secondary AS and that the database is unlocked:

```
<#root>
$
repctl status
$
peerctl unlock
```

Check `healthmon -l` on all ASs. Ensure the reported severity is NOTIFICATION for all servers.

Verify that the secondary AS and primary AS databases are synchronized (on secondary):

```
<#root>
```

```
$
```

```
synchcheck_basic.pl -a
```

## Secondary AS Upgrade Switch

Start the upgrade by entering this command:

```
<#root>
```

```
AS_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server AS 2023.03_1.411
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of AS to 2023.03_1.411. NOTE that this action will  
Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

Update the database statistics by running the `bwPeriodMaint.sh` script:

```
<#root>
```

```
$
```

```
bwPeriodMaint.sh
```

## Secondary AS Post-Upgrade Actions

### AS Post-Upgrade Checks

Post upgrade, check the AS status after startup and verify registrations and calls.

- `healthmon -l`
- `showrun`
- `bwshowver`
- Review `/var/broadworks/logs/maintenance/ setactiveserver.AS.Rel_2023.03_1.411.<date-time>.log` file for any potential activation errors.
- Run AS tests in order to ensure that this AS is processing calls properly.

## Recommended AS Post-Upgrade Tests

- Lock the Primary AS to force new calls to the secondary.
- Validate SIP outbound calling.
- Validate MGCP outbound calling.
- Validate PSTN to SIP user inbound calling.
- Validate PSTN to MGCP user inbound calling.
- Validate voice mail leaving/retrieval (voice portal).
- Validate CommPilot originations/terminations.
- Validate CLI access (go to AS\_CLI/System/Alias and use the get command).
- Validate direct web access to the AS.

## Post-Cluster Test

- Ensure healthmon reports severity NOTIFICATION for all servers.
- Check database synchronization:

```
<#root>
$
healthmon -l
$
synchcheck_basic.pl â€"a
```

## Service Control Function (SCF)

Ensure healthmon shows no issues:

```
-----
System Health Report Page
BroadWorks Server Name: scf1
Date and time      : Fri Nov  8 11:30:38 GMT 2022
Report severity    : NOTIFICATION
Server type        : ServiceControlFunction
Server state       : Unlock
-----
```

No abnormal condition detected.

- Check the logs to ensure the SCF is processing calls.

## Backup and Tech-Support

Prior to any server upgrade, it is recommended to take a backup and log a tech-support from prior to



upgrade. This is done with:

```
<#root>
$
bwAutoBackup.sh
$
tech-support
  >> tsup_hostname_sourceRelease.txt
```

## Pre-Upgrade

Test calls from the Mobile network in order to ensure current function is working as normal.

Run the upgradeCheck tool in order to ensure no warnings are issued:

```
<#root>
SCF_CLI/Maintenance/Tools>
upgradeCheck SCF_Re1_2023.03_1.411
```

If a redundant setup, lock the server to force calls to the other SCF:

```
<#root>
SCF_CLI/Maintenance/ManagedObjects>
lock
```

## SCF Upgrade Switch

Once the calls have dropped to an acceptable level, start the upgrade with:

```
<#root>
SCF_CLI/Maintenance/ManagedObjects>
set activeSoftwareVersion server SCF 2023.03_1.411

+++ WARNING +++ WARNING +++ WARNING +++
This command will change the active software version of SCF to 2023.03_1.411. NOTE that this action will
Continue?

Please confirm (Yes, Y, No, N):
y
```

Once complete, unlock the server and test calls:

```
<#root>
```

```
SCF_CLI/Maintenance/ManagedObjects>
```

```
unlock
```

## SCF Post-Upgrade Checks

Post upgrade, check the SS7 logs for a good startup:

- **healthmon -l**
- **showrun**
- **bwshowver**
- Review `/var/broadworks/logs/maintenance/ setactiveserver.SCF.Rel_2023.03_1.411.<date-time>.log` file for any potential activation errors.
- Run tests to ensure that this SCF is processing calls properly.
- Confirm calls from mobile network to the BroadWorks core are working as before the upgrade.

## SCF Server Revert

In the event that the SCF does not pass the post upgrade checks, revert back to the previous release:

```
<#root>
```

```
SCF_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server SCF 2022.10_1.313 revert
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of SCF to 2022.10_1.313. NOTE that this action will  
Continue?
```

```
Please confirm (Yes, Y, No, N):
```

```
y
```

In the example, it is reverting back to 2022.10\_1.313 but this can be substituted for any previous release.

## Application Delivery Platform (ADP)

Ensure healthmon shows no issues:

```
-----  
System Health Report Page
```

```
BroadWorks Server Name: adp1
```

```
Date and time      : Fri Nov  8 11:30:38 GMT 2022
```

Report severity : NOTIFICATION  
Server type : ApplicationDeliveryPlatform  
Server state : Unlock

---

No abnormal condition detected.

---

## Backup and Tech-Support

Prior to any server upgrade, it is recommended to take a backup and log a tech-support from prior to upgrade. This would be done with:

```
<#root>  
  
$  
  
bwAutoBackup.sh  
  
$  
  
tech-support  
  
>> tsup_hostname_sourceRelease.txt
```

## Pre-Upgrade

Run the upgradeCheck tool to ensure no warnings are issued:

```
<#root>  
  
ADP_CLI/Maintenance/Tools>  
  
upgradeCheck ADP_Rel_2022.10_1.313
```

Lock the server prior to activation of the new software version:

```
<#root>  
  
ADP_CLI/Maintenance/ManagedObjects>  
  
lock
```

## Undeploy and Deactivate ECLQuery Application When Moving from ADP/PS on R23 to RI

Before we upgrade the ADP to the latest RI, we need to migrate the ECLQuery application to the NDS IF the source ADP/PS on R23 has ECLQuery application running. Refer to to [Enhanced Call Log Migration](#)

[from Database Server to Network Database Server Feature Description.](#)

```
<#root>
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
undeploy application /ECLQuery
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
deactivate application /ECLQuery
```

If this is not done, we see a `CentralizedDatabaseListenerFailure` alarm on the ADP after activation of the new release.

## Upload the ADP RI/RA Applications Matching the Deployed Applications on the Source Release

The ADP BroadWorks server requires that the RI/RA versions of the applications currently deployed on the source release are downloaded from Cisco.com. In order to get the list of required applications, complete these actions.

On the ADP, enter:

```
<#root>
```

```
$
```

```
bwshowver
```

```
ADP version Rel_2022.11_1.273
```

```
Applications Info:
```

- OpenClientServer version 2022.11\_1.273
- WebContainer version 2022.11\_1.273
- OCIOverSoap version 2022.11\_1.273 context path /webservice
- CommPilot version 2022.11\_1.273 context path /
- Xsi-Actions version 2022.11\_1.273 context path /com.broadsoft.xsi-actions
- Xsi-Events version 2022.11\_1.273 context path /com.broadsoft.xsi-events
- Xsi-VTR version 2022.11\_1.273 context path /vtr
- OCIFiles version 2022.11\_1.273 context path /ocifiles
- BroadworksDms version 2022.11\_1.273 context path /dms
- AuthenticationService version 2022.11\_1.273 context path /authservice

All applications listed after the `Applications Info` are applications that are deployed on the ADP and require downloading the ADP compatible versions from Cisco.com. Download the latest versions available. Examples of the applications based on the previous example are as follows:

```
OCS_2023.01_1.193.bwar
```

```
OCIOverSoap_2023.01_1.193.bwar
```

Xsi-Actions-24\_2023.01\_1.010.bwar

Xsi-Events-24\_2023.01\_1.010.bwar

CommPilot-24\_2023.01\_1.010.bwar

Xsi-VTR-24\_2023.01\_1.010.bwar

OCIFiles\_2023.01\_1.010.bwar

dms\_2023.01\_1.193.bwar

Copy the downloaded bwar / war files to the ADP and placed in the /usr/local/broadworks/apps directory:

```
<#root>
```

```
$
```

```
cd <bwar / war directory location>
```

```
$
```

```
cp OCS_2023.01_1.193.war /usr/local/broadworks/apps/
```

```
$ <Repeat for every application>
```

The rest of the upgrade is a normal BroadWorks upgrade.

## Pre-Upgrade

Run the upgradeCheck tool in order to ensure no warnings are issued:

```
<#root>
```

```
ADP_CLI/Maintenance/Tools>
```

```
upgradeCheck ADP_Rel_2023.03_1.411
```

## ADP Upgrade Switch

Start the upgrade by entering this command:

```
<#root>
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server ADP 2023.03_1.411
```

```
+++ WARNING +++ WARNING +++ WARNING +++
```

```
This command will change the active software version of ADP to 2023.03_1.411. NOTE that this action will  
Continue?
```

Please confirm (Yes, Y, No, N):

## ADP Post-Upgrade Actions

### Upgrade Applications

The WebContainer application is automatically upgraded. The other applications fall into two types, Cisco BroadWorks applications and web applications. The upgrade procedure is different depending on if the application is a Cisco BroadWorks application or a web application.

- Cisco BroadWorks applications are packaged as a BroadWorks ARchive (.bwar) file.
- Web applications, packaged as Web ARchive (.war) file.

Enter the `qbw` command to see what version is currently active for each application and its deployed context path.

### Upgrade Web Applications

Web applications are upgraded by deactivating and undeploying the current version, then activating and deploying the new version:

```
<#root>
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
undeploy application /callcenter
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
deactivate application /callcenter
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
activate application BWCallCenter 2023.04_1.150 /callcenter
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
deploy application /callcenter
```

### Upgrade Cisco BroadWorks Applications

Cisco BroadWorks Applications are upgraded from the bwcli using the `set activeSoftwareVersion application` command.

More details can be found in the [Applications Release Notes](#) and the [Application Deployment Platform Config Guide](#).

```
<#root>
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion application LoadBalancer 2023.02_1.090
```

+++ WARNING +++ WARNING +++ WARNING +++ Upgrading an application will cause downtime for the targeted co

Please confirm (Yes, Y, No, N):

y

--> Stopping application LoadBalancer <--

Stopping [done]

BroadWorks SW Manager upgrading LoadBalancer to version 2023.02\_1.090 ...Done

## Roll Back ADP Applications

If, for some reason, the application must be rolled back to a previous version, the process is similar to an upgrade. One important thing to note is that some changes might be lost after the rollback operation is executed (for example, configuration changes) because the resulting active application is in the state it was before the upgrade.

## Roll Back Web Applications

Web applications are reverted by deactivating and undeploying the current version, then activating and deploying the new version:

```
<#root>
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
undeploy application /callcenter
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
deactivate application /callcenter
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
activate application BWCallCenter 2023.04_1.150 /callcenter
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
deploy application /callcenter
```

## Rollback Cisco BroadWorks Applications

Cisco BroadWorks Applications are reverted from the bwcli using the `set activeSoftwareVersion application` command:

```
<#root>
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion application LoadBalancer 2020.09_1.090
```

+++ WARNING +++ WARNING +++ WARNING +++ Upgrading an application will cause downtime for the targeted co

Please confirm (Yes, Y, No, N):

y

--> Stopping application LoadBalancer <--

Stopping [done]

BroadWorks SW Manager upgrading LoadBalancer to version 2020.09\_1.090 ...Done

## ADP Post-Upgrade Checks

Post upgrade, check the logs for a good startup and log in to GUI as before.

- **healthmon -l**
- **showrun**
- **bwshowver**
- Review /var/broadworks/logs/maintenance/ setactiveserver.ADP.Rel\_2023.03.0\_1.1411.<date-time>.log file for any potential activation errors.

## Recommended ADP Post-Upgrade Tests

- Verify administrator level login.
- Verify user level login.
- Validate CommPilot Call Manager functionality.
- Validate Call Control Client (for example, BroadWorks Assistant-Enterprise) and Operations Support System (OSS)/Open Client Interface (OCI) functionality.
- Validate that any Open Client Server (OCS) proxy provisioning to the AS or NS is functioning properly.

These tests are generic, run any additional tests in the post-upgrade test plan.

## ADP Server Revert

If the ADP does not pass the post upgrade check, revert to the previous release:

```
<#root>
```

```
ADP_CLI/Maintenance/ManagedObjects>
```

```
set activeSoftwareVersion server ADP 2022.10_1.313 revert
```

+++ WARNING +++ WARNING +++ WARNING +++

This command will change the active software version of ADP to 2022.10\_1.313. NOTE that this action will  
Continue?

Please confirm (Yes, Y, No, N):

y

In the example, it is reverting back to 2022.10\_1.313 but this can be substituted for any previous release.