



VOSS Automate Upgrade Guide with Delta Bundle

Release 21.2

Feb 08, 2022

Legal Information

Please take careful note of the following legal notices:

- Copyright © 2022 VisionOSS Limited.
All rights reserved.
- VOSS, VisionOSS and VOSS Automate are trademarks of VisionOSS Limited.
- No part of this document may be reproduced or transmitted in any form without the prior written permission of VOSS.
- VOSS does not guarantee that this document is technically correct, complete, or that the product is free from minor flaws. VOSS endeavors to ensure that the information contained in this document is correct, whilst every effort is made to ensure the accuracy of such information, VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.
- This document is used entirely at the users own risk. VOSS cannot be held responsible or liable for any damage to property, loss of income, and or business disruption arising from the use of this document.
- The product capabilities described in this document and the actual capabilities of the product provided by VOSS are subject to change without notice.
- VOSS reserves the right to publish corrections to this document whenever VOSS deems it necessary.
- All vendor/product names mentioned in this document are registered trademarks and belong to their respective owners. VOSS does not own, nor is related to, these products and vendors. These terms have been included to showcase the potential of the VOSS solution and to simplify the deployment of these products with VOSS should you select to utilize them.

Security Information

This product may contain cryptographic features that may be subject to state and local country laws that govern the import, export, transfer and use of such features. The provision of this software does not imply that third-party authorization to import, export, distribute or use encryption in your particular region has been obtained. By using this product, you agree to comply with all applicable laws and regulations within your region of operation. If you require further assistance, please contact your dedicated VOSS support person.

Contents

1	Using the <code>screen</code> command	2
2	Multinode Upgrade	4
2.1	Unified Node Topology: Upgrade a Multinode Environment with the Delta Bundle	4
2.2	Modular Cluster Topology: Upgrade a Multinode Environment with the Delta Bundle	11
3	Single Node Upgrade	19
3.1	Upgrade a Single Node Cluster Environment with the Delta Bundle	19
	Index	25

Note:

- Normal operations will be interrupted during an upgrade. Carry out the upgrade in a maintenance window. Refer to the type of upgrade for details on the upgrade duration.
- Users on Azure who carry out this Delta bundle upgrade should first install the patch file: `EKB-11598-21.1_patch.script`:

The Patch and the MOP are available here:

- Server Name: <https://voss.portalshape.com>
 - Path: **Downloads > VOSS-4-UC > 21.1 > Patches**
 - Patch Directory: **EKB-11598-21.1_patch**
 - Patch File: `EKB-11598-21.1_patch.script`
 - MOP File: `MOP-EKB-11598-21.1_patch.pdf`
-

Note: From release 21.1 onwards, a new field called **Usage** has been added to Directory Numbers (DN). This field tracks the type of device which the DN has been assigned to. For example: for Phones, Device Profiles and Remote Destination Profiles the usage is “Device”. For Hunt Groups, the usage is “Hunt_Pilot”, and so on.

The **Usage** field is automatically populated when the DNs are assigned to and removed from various devices from 21.1 onwards.

In order to populate the **Usage** field once-off for all existing Directory Number inventory instances, the Audit Number Inventory tool should be run once post-upgrade for each customer.

The tool only needs to be run once when initially upgrading to a 2x.x release from a 18.x or 19.x release. If it was already run when upgrading to 21.1 for example, then it does not need to be run again when upgrading later versions, for example 21.2, 21.3, 22.1, and so on.

Before running the tool:

- Careful consideration must be taken when selecting where the Number Inventory is deployed: Customer or Site - this is usually Dial Plan dependent.
 - Please review the Audit Number Inventory topic in the Core Feature Guide.
-

1. Using the `screen` command

The **screen** command is available to execute long-running commands (for example, when upgrading) in the background.

The following commands require the running of **screen**:

- **cluster provision**
- **cluster upgrade**
- **app template**
- **voss export type <args>**
- **voss export group <args>**
- **voss subscriber_data_export**

A message is displayed to indicate that **screen** should be run first:

```
This is a potentially long-running command and should be executed in a screen session
Run `screen` and then execute the command again
```

The use of **screen** is *not affected* by the use of the `--force` parameter with any of these commands.

The commands then run in a screen session that can be reconnected. The standard screen command parameters are available, in particular:

- **screen** - start a new session
- **screen -ls** - show sessions already available
- **screen -r [screen PID]** - reconnect to a disconnected session

The version of **screen** used in VOSS Automate also supports the creation of a log file. If long-running commands will be run, the log file captures screen console output up to the session timeout. A message shows:

```
timed out waiting for input: auto-logout
```

To create a screen log file:

1. Run **screen** and wait for screen to open.
2. Press **<Ctrl>-a** then **:** (colon). This will enter screen command mode at the bottom of the console.
3. Create your screen logfile in the `media/` directory:
 - a. In screen command mode, type **logfile media/<screen-logfilename>.log**
 - b. Press **<Enter>**
 - c. Press **<Ctrl>-a** and then **H** to start writing to the log file

d. Run your commands.

If the **screen** session times out, you can obtain console output from the log file, for example:

\$ sftp platform@<host>:media/<screen-logfilename>.log

2. Multinode Upgrade

2.1. Unified Node Topology: Upgrade a Multinode Environment with the Delta Bundle

Note:

- While system upgrade takes approximately two hours at a single site, this may vary in accordance with your topology, number of devices and subscribers. Adjust your upgrade maintenance window to allow for your configuration.
-

The standard **screen** command should be used where indicated, and the *reconnect* parameter is available if needed:

- **screen** - start a new session
- **screen -ls** - show sessions already available
- **screen -r [screen PID]** - reconnect to a disconnected session

We recommend using the **screen** command to avoid failures if the connection is interrupted whilst running the command. If the connection is interrupted whilst running the command in `screen` then the session can be retrieved by first listing the sessions PID currently running in `screen`: **screen -ls**, and then reconnecting to the session using **screen -r [screen PID]**.

The version of **screen** used in VOSS Automate also supports the creation of a log file. If long-running commands will be run, the log file captures screen console output up to the session timeout. A message shows:

```
timed out waiting for input: auto-logout
```

To create a screen log file:

1. Run **screen** and wait for screen to open.
2. Press **<Ctrl>-a** then **:** (colon). This will enter screen command mode at the bottom of the console.
3. Create your screen logfile in the `media/` directory:
 - a. In screen command mode, type **logfile media/<screen-logfilename>.log**
 - b. Press **<Enter>**
 - c. Press **<Ctrl>-a** and then **H** to start writing to the log file
 - d. Run your commands.

If the **screen** session times out, you can obtain console output from the log file, for example:

```
$ sftp platform@<host>:media/<screen-logfilename>.log
```

2.1.1. Download Files and Check

Description and Steps	Notes and Status
<p>VOSS files: https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade Download XXX-Delta-Bundle.script file, where XXX matches the release. Transfer the XXX-Delta-Bundle.script file to the media/ folder of the primary Unified node. Two file transfer options: Either using SFTP:</p> <ul style="list-style-type: none"> • sftp platform@<primary_unified_node_hostname> • cd media • put <XXX-Delta-Bundle.script> <p>Or using SCP:</p> <ul style="list-style-type: none"> • scp <XXX-Delta-Bundle.script> platform@<primary_unified_node_hostname>:~/media <p>On the primary Unified node, verify that the .script file copied:</p> <ul style="list-style-type: none"> • ls -l media/ <p>On the primary Unified node, verify that the original .sha256 checksums on the SFTP server match.</p> <ul style="list-style-type: none"> • system checksum media/<XXX-Delta-Bundle.script> Checksum: <SHA256> 	

2.1.2. Adaptations Check

Description and Steps	Notes and Status
<p>Identify installed adaptations and determine any effect on the upgrade plan. If the release is accompanied by Upgrade Notes, refer to the details.</p>	

2.1.3. Schedules, Transactions and Version Check

Description and Steps	Notes and Status
<p>Turn off any scheduled imports to prevent syncs triggering part way through the upgrade. Two options are available:</p> <p>Individually for each job:</p> <ol style="list-style-type: none"> 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the Scheduling menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, uncheck the Activate check box. <p>Mass modify:</p> <ol style="list-style-type: none"> 1. On the GUI, export scheduled syncs into a bulk load sheet. 2. Modify the schedule settings to de-activate scheduled syncs. 3. Import the sheet. <p>Schedules enabled on the CLI:</p> <ol style="list-style-type: none"> 1. Run schedule list to check if any schedules exist and overlap with the maintenance window. 2. For overlapping schedules, disable. Run schedule disable <job-name>. 	
<p>Check for running imports. Either wait for them to complete or cancel them:</p> <ol style="list-style-type: none"> 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the Transaction menu to view transactions. 3. Filter the Action column: <ol style="list-style-type: none"> a. Choose Status as "Processing" and then choose each Action that starts with "Import", for example, "Import Unity Connection". b. Click Search and confirm there are no results. c. If there are transactions to cancel, select them and click Cancel. 	
<p>Customized ``data/Settings``</p> <p>If <code>data/Settings</code> instances have been modified, record these or export them as JSON. The modifications can be re-applied or exported JSON instances can be merged following the upgrade. See: Post Template Upgrade Tasks.</p> <p>Version</p> <p>Record the current version information. This is required for upgrade troubleshooting.</p> <ul style="list-style-type: none"> • Log in on the GUI and record the information contained in the About > Extended Version 	

2.1.4. Pre-Upgrade, Security and Health Steps

Description and Steps	Notes and Status
<p>Verify that the primary node is the active primary node at the time of upgrade.</p> <p>database config</p> <p>Ensure that the node on which the installation will be initiated has the <code>stateStr</code> parameter set to PRIMARY and has the highest <code>priority number</code> (highest priority number could vary depending on cluster layout).</p> <p>Example output</p> <pre><ip address>:27020: priority: <number> stateStr: PRIMARY storageEngine: WiredTiger</pre> <p>Validate the system health.</p> <p>On the Primary Unified Node, verify cluster connectivity:</p> <ul style="list-style-type: none"> • cluster status <p>On each node verify network connectivity, disk status and NTP.</p> <ul style="list-style-type: none"> • cluster check <p>If there is any sign of the paths below are over 80% full, a clean-up is needed to avoid risk of for example full logs occurring during upgrade. Clean-up steps are indicated next to the paths:</p> <pre>/ (call support if over 80%) /var/log (run: log purge) /opt/platform (remove any unnecessary files from /media directory) /tmp (reboot)</pre> <p>On the Primary Unified Node, verify there are no pending Security Updates on any of the nodes:</p> <ul style="list-style-type: none"> • cluster run all security check 	
<p>As part of the rollback procedure, ensure that a suitable restore point is obtained prior to the start of the activity, as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.</p> <p>VOSS cannot guarantee that a restore point can be used to successfully restore VOSS Automate. If you cannot restore the application from a restore point, your only recourse is to reinstall the application.</p> <p>Optional: If a backup is also required, use the backup add <location-name> and backup create <location-name> commands. For details, refer to the Platform Guide.</p>	

Description and Steps	Notes and Status
<p>Before upgrading, check all services, nodes and weights for the cluster: Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh unified nodes.</p> <ul style="list-style-type: none"> • cluster run all app status <p>Make sure all application nodes show 3 or 5 nodes.</p> <ul style="list-style-type: none"> • cluster run application cluster list <p>Check that the database weights are set. It is <i>critical</i> to ensure the weights are set before upgrading a cluster.</p> <ul style="list-style-type: none"> • cluster run application database weight list <p>Example output:</p> <pre>172.29.21.240: weight: 80 172.29.21.241: weight: 70 172.29.21.243: weight: 60 172.29.21.244: weight: 50</pre> <p>Verify the primary node in the primary site and ensure no nodes are in the 'recovering' state (<code>stateStr</code> is not <code>RECOVERING</code>). On the primary node:</p> <ul style="list-style-type: none"> • database config 	

2.1.5. Upgrade

Description and Steps	Notes and Status
<p>On the primary unified node:</p> <ul style="list-style-type: none"> • screen <p>Run (optionally with command parameters below):</p> <ul style="list-style-type: none"> • app install media/<script_file> delete-on-success yes -force <p>The upgrade will also silently run an updated version of cluster check and the upgrade will fail to proceed if any error conditions exist. Fix before proceeding. Refer to the Platform Guide for details on the new version of the cluster check command.</p> <p>Run:</p> <ul style="list-style-type: none"> • database config <p>and verify the number of nodes are <i>uneven</i>, i.e. either 5 or 7. If not, run: cluster provision role database and ensure an arbitrator shows when you run database config again (<code>stateStr: ARBITER</code>).</p> <p>From release 19.1.2 and later, the <code>delete-on-success</code> parameter and <code>yes</code> or <code>no</code> value have been added to remove or keep the the script file in the <code>media/</code> directory after successful installation.</p> <p>Note that during the upgrade, phone registration data is cleared. A message will show in the log: <code>Remove phone registration data</code>. This is required so that old values are not displayed, since after the upgrade this information is no longer stored in the resource cache.</p>	

2.1.6. Post-Upgrade, Security and Health Steps

Description and Steps	Notes and Status
<p>On the primary unified node, verify the cluster status:</p> <ul style="list-style-type: none"> • cluster status • cluster check • If any of the above commands show errors, check for further details to assist with troubleshooting: cluster run all diag health 	
<p>If upgrade is successful, the screen session can be closed by typing exit in the screen terminal. If errors occurred, keep the screen terminal open for troubleshooting purposes and contact VOSS support.</p>	
<p>Check for needed security updates. On the primary node, run:</p> <ul style="list-style-type: none"> • cluster run all security check <p>If one or more updates are required for any node, run on the primary Unified node:</p> <ul style="list-style-type: none"> • cluster run all security update <p>Note: <i>if the system reboots, do not carry out the next manual reboot step.</i> Manual reboot <i>only if needed</i>:</p> <ul style="list-style-type: none"> • cluster run notme system reboot <p>If node messages: <code><node name> failed with timeout</code> are displayed, these can be ignored.</p> <ul style="list-style-type: none"> • system reboot <p>Since all services will be stopped, this takes some time.</p>	

2.1.7. Post Template Upgrade Tasks

Description and Steps	Notes and Status
<p>Customized ``data/Settings`` Merge the previously backed up customized <code>data/Settings</code> with the latest settings on the system by manually adding the differences or exporting the latest settings to JSON, merging the customized changes and importing the JSON.</p> <p>Support for VG400 and VG450 Analogue Gateways Before adding the VG400 or VG450 Gateway, the <code>device/cucm/GatewayType</code> model needs to be imported for each Unified CM.</p> <ol style="list-style-type: none"> 1. Create a Model Type List which includes the <code>device/cucm/GatewayType</code> model. 2. Add the Model Type List to all the required Unified CM Data Syncs. 3. Execute the Data Sync for all the required Unified CMs. <p>Verify the upgrade Log in on the GUI and check the information contained in the About > Extended Version menu. Confirm that versions have upgraded:</p> <ul style="list-style-type: none"> • Release should show 21.2 • Platform Version should show 21.2 <p>If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again.</p>	
<ul style="list-style-type: none"> • For configurations that make use of the Northbound Billing Integration (NBI), please check the service status of NBI and restart if necessary. 	

2.1.8. Restore Adaptations

Description and Steps	Notes and Status
Restore and adaptations prior to upgrade. If the release is accompanied by Upgrade Notes, refer to the details on adaptation impact.	

2.1.9. Restore Schedules

Description and Steps	Notes and Status
<p>Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available:</p> <p>Individually for each job:</p> <ol style="list-style-type: none"> 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the Scheduling menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, check the Activate check box. <p>Mass modify:</p> <ol style="list-style-type: none"> 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the bulk load sheet. <hr/> <p>Note: Select the Skip next execution if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter.</p> <hr/> <p>Schedules enabled on the CLI:</p> <ol style="list-style-type: none"> 1. For disabled schedules that were overlapping the maintenance window, enable. Run schedule enable <job-name>. 	

For overlapping schedules, disable. Run **schedule disable <job-name>**.

2.1.10. Log Files and Error Checks

Description and Steps	Notes and Status
<p>Inspect the output of the command line interface for upgrade errors.</p> <p>Use the log view command to view any log files indicated in the error messages, for example, run the command if the following message appears:</p> <pre>For more information refer to the execution log file with 'log view platform/execute.log'</pre> <p>For example, if it is required send all the install log files in the <code>install</code> directory to an SFTP server:</p> <ul style="list-style-type: none"> • log send sftp://x.x.x.x install 	
<p>Log in on the GUI as system level administrator, go to Administration Tools > Transaction and inspect the transactions list for errors.</p>	

2.2. Modular Cluster Topology: Upgrade a Multinode Environment with the Delta Bundle

Note:

- While system upgrade takes approximately two hours at a single site, this may vary in accordance with your topology, number of devices and subscribers. Adjust your upgrade maintenance window to allow for your configuration.

The standard **screen** command should be used where indicated. See: [Using the screen command](#).

2.2.1. Determine the Primary database and application node in a Modular Cluster Topology

Important: All upgrade steps are to be run from the *primary application node*. Where it is necessary to run database node commands from this application node, the primary database node IP will be passed in as a parameter with the command.

In order to run the commands for the upgrade on the nodes with the appropriate roles, determine:

- The *primary application node*
- The *primary database node*

1. Log in on a node in your modular cluster.
2. To find the *primary application node* in the cluster:

```
$ cluster run all cluster primary role application
```

Record the node entry where `is_primary: true`, for example:

```
----- VOSS-UN-1, ip=192.168.100.3, role=webproxy,application, loc=cpt
is_primary: true
```

3. To find the *primary database node* in the cluster:

```
$ cluster run all cluster primary role database
```

Record the node entry IP where `is_primary: true`, for example:

```
----- VOSS-UN-2, ip=192.168.100.4, role=database, loc=cpt
is_primary: true
```

This IP address will be used in command parameters during upgrade.

Note: When the **cluster run all primary role <role>** command is run, web proxy nodes will return a failure - this can be ignored. For example:

```
----- VOSS-WP-1, ip=192.168.100.9, role=webproxy, loc=cpt
Invalid command syntax - refer to help descriptions
```

2.2.2. Download Files and Check

Description and Steps	Notes and Status
<p>VOSS files: https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade Download XXX-Delta-Bundle.script file, where XXX matches the release. Transfer the XXX-Delta-Bundle.script file to the media/ folder of the primary application node. Two file transfer options: Either using SFTP: <ul style="list-style-type: none"> • sftp platform@<primary_application_hostname> • cd media • put <XXX-Delta-Bundle.script> Or using SCP: <ul style="list-style-type: none"> • scp <XXX-Delta-Bundle.script> platform@<primary_application_hostname>:~/media On the primary application node, verify that the .script file copied: <ul style="list-style-type: none"> • ls -l media/ On the primary application node, verify that the original .sha256 checksums on the Download site match. <ul style="list-style-type: none"> • system checksum media/<XXX-Delta-Bundle.script> Checksum: <SHA256> </p>	<p></p>

2.2.3. Adaptations Check

Description and Steps	Notes and Status
<p>Identify installed adaptations and determine any effect on the upgrade plan. If the release is accompanied by Upgrade Notes, refer to the details.</p>	<p></p>

2.2.4. Schedules, Transactions and Version Check

Description and Steps	Notes and Status
<p>Turn off any scheduled imports to prevent syncs triggering part way through the upgrade. Two options are available:</p> <p>Individually for each job:</p> <ol style="list-style-type: none"> 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the Scheduling menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, uncheck the Activate check box. <p>Mass modify:</p> <ol style="list-style-type: none"> 1. On the GUI, export scheduled syncs into a bulk load sheet. 2. Modify the schedule settings to de-activate scheduled syncs. 3. Import the sheet. <p>Schedules enabled on the CLI: on the primary application node:</p> <ol style="list-style-type: none"> 1. Check if any schedules exist. Run: cluster run all schedule list Record the IP addresses of nodes with schedules overlapping with the maintenance window. 2. For overlapping schedules on a node, disable. Run: cluster run <node IP> schedule disable <job-name> 	
<p>Check for running imports. Either wait for them to complete or cancel them:</p> <ol style="list-style-type: none"> 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the Transaction menu to view transactions. 3. Filter the Action column: <ol style="list-style-type: none"> a. Choose Status as "Processing" and then choose each Action that starts with "Import", for example, "Import Unity Connection". b. Click Search and confirm there are no results. c. If there are transactions to cancel, select them and click Cancel. 	
<p>Customized ``data/Settings``</p> <p>If <code>data/Settings</code> instances have been modified, record these or export them as JSON. The modifications can be re-applied or exported JSON instances can be merged following the upgrade. See: Post Template Upgrade Tasks.</p> <p>Version</p> <p>Record the current version information. This is required for upgrade troubleshooting.</p> <ul style="list-style-type: none"> • Log in on the GUI and record the information contained in the About > Extended Version 	

2.2.5. Pre-Upgrade, Security and Health Steps

Description and Steps	Notes and Status
<p>Have the IP address available of the node determined to be the <i>primary database node</i>. Verify that the primary database node is the active primary node at the time of upgrade. On the primary application node, run:</p> <p>cluster run <primary db IP> database config</p> <p>From the output, ensure that the primary database node <code>stateStr</code> parameter is set to PRIMARY and it has the <i>highest</i> <code>priority:<number></code> (highest priority number could vary depending on cluster layout).</p> <p>Example output</p> <pre><ip address>:27020: priority: <number> stateStr: PRIMARY storageEngine: WiredTiger</pre> <p>Validate the system health on the primary application node:</p> <p>Verify cluster connectivity</p> <ul style="list-style-type: none"> • cluster run all cluster status <p>Verify network connectivity, disk status and NTP.</p> <ul style="list-style-type: none"> • cluster check verbose <p>If there is any sign of the paths below are over 80% full, a clean-up is needed to avoid risk of for example full logs occurring during upgrade. Clean-up steps are indicated next to the paths:</p> <pre>/ (call support if over 80%) /var/log (run: log purge) /opt/platform (remove any unnecessary files from /media directory) /tmp (reboot)</pre> <p>On the primary application node, verify there are no pending Security Updates on any of the nodes:</p> <ul style="list-style-type: none"> • cluster run all security check 	
<p>As part of the rollback procedure, ensure that a suitable restore point is obtained prior to the start of the activity, as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed. VOSS cannot guarantee that a restore point can be used to successfully restore VOSS Automate. If you cannot restore the application from a restore point, your only recourse is to reinstall the application.</p> <p>Optional: If a backup is also required</p> <ul style="list-style-type: none"> • Application node backup: <p>On the primary application node, use the backup add <location-name> and backup create <location-name> commands. For details, refer to the Platform Guide.</p> • Database node backup: <ul style="list-style-type: none"> – Find the database node with the <i>second</i> highest weight. On the primary application node, run cluster run database database weight list to find this node. – Log in on the database node with the <i>second</i> highest weight. – Run backup add <location-name> and backup create <location-name> commands. For details, refer to the Platform Guide. 	

Description and Steps	Notes and Status
<p>Before upgrading, check all services, nodes and weights for the cluster on the primary application node.</p> <p>Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh database nodes.</p> <ul style="list-style-type: none"> • cluster run all app status <p>Make sure all application nodes show.</p> <ul style="list-style-type: none"> • cluster run application cluster list <p>Check that the database weights are set. It is <i>critical</i> to ensure the weights are set before upgrading a cluster. The command is run from the primary application node and is carried out on all database nodes</p> <ul style="list-style-type: none"> • cluster run database database weight list <p>Example output:</p> <pre>----- VOSS-UN-2, ip=192.168.100.4, role=database, loc=cpt 192.168.100.4: weight: 70 192.168.100.6: weight: 50 192.168.100.8: weight: 30 ----- VOSS-UN-4, ip=192.168.100.6, role=database, loc=cpt [...]</pre> <p>Verify the primary database node in the primary site and ensure no nodes are in the 'recovering' state (<code>stateStr</code> is not <code>RECOVERING</code>). Run on the primary application node and use the primary database IP as parameter:</p> <ul style="list-style-type: none"> • cluster run <primary db IP> database config 	

2.2.6. Upgrade

Description and Steps	Notes and Status
<p>On the primary application node:</p> <ul style="list-style-type: none"> • screen <p>Run (optionally with command parameters below):</p> <ul style="list-style-type: none"> • app install media/<script_file> delete-on-success yes -force <p>The upgrade will also silently run an updated version of cluster check and the upgrade will fail to proceed if any error conditions exist. Fix before proceeding. Refer to the Platform Guide for details on the new version of the cluster check command.</p> <p>Run on the primary application node and use the primary database IP as parameter:</p> <ul style="list-style-type: none"> • cluster run <primary db IP> database config <p>and verify the number of nodes are <i>uneven</i>, i.e. either 5 or 7. If not, run:</p> <ul style="list-style-type: none"> • cluster run <primary db IP> cluster provision role database <p>Ensure an arbitrator shows when you run the command again:</p> <ul style="list-style-type: none"> • cluster run <primary db IP> database config <p>(output shows: <code>stateStr: ARBITER</code>)</p> <p>Note that during the upgrade, phone registration data is cleared. A message will show in the log: <code>Remove phone registration data</code>. This is required so that old values are not displayed, since after the upgrade this information is no longer stored in the resource cache.</p>	

2.2.7. Post-Upgrade, Security and Health Steps

Description and Steps	Notes and Status
<p>On the primary application node, verify the cluster status:</p> <ul style="list-style-type: none"> • cluster status • cluster check <p>If any of the above commands show errors, check for further details to assist with troubleshooting:</p> <ul style="list-style-type: none"> • cluster run all diag health 	
<p>If upgrade is successful, the screen session can be closed by typing exit in the screen terminal. If errors occurred, keep the screen terminal open for troubleshooting purposes and contact VOSS support.</p>	
<p>Check for needed security updates. On the primary application node, run:</p> <ul style="list-style-type: none"> • cluster run all security check <p>If one or more updates are required for any node, run on the primary application node:</p> <ul style="list-style-type: none"> • cluster run all security update <p>Note: <i>if the system reboots, do not carry out the next manual reboot step.</i></p> <p>Manual reboot <i>only if needed</i>:</p> <ul style="list-style-type: none"> • cluster run notme system reboot <p>If node messages: <code><node name> failed with timeout</code> are displayed, these can be ignored.</p> <ul style="list-style-type: none"> • system reboot <p>Since all services will be stopped, this takes some time.</p>	

2.2.8. Post Template Upgrade Tasks

Description and Steps	Notes and Status
<p>Customized ``data/Settings`` For releases prior to 21.1, merge the previously backed up customized <code>data/Settings</code> with the latest settings on the system by manually adding the differences or exporting the latest settings to JSON, merging the customized changes and importing the JSON.</p> <p>Support for VG400 and VG450 Analogue Gateways Before adding the VG400 or VG450 Gateway, the <code>device/cucm/GatewayType</code> model needs to be imported for each Unified CM.</p> <ol style="list-style-type: none"> 1. Create a Model Type List which includes the <code>device/cucm/GatewayType</code> model. 2. Add the Model Type List to all the required Unified CM Data Syncs. 3. Execute the Data Sync for all the required Unified CMs. <p>Verify the upgrade Log in on the GUI and check the information contained in the About > Version menu. Confirm that versions have upgraded:</p> <ul style="list-style-type: none"> • Release should show <code>xxx</code> where <code>xxx</code> corresponds with the release number of the upgrade. <p>If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again.</p>	
<ul style="list-style-type: none"> • For configurations that make use of the Northbound Billing Integration (NBI), please check the service status of NBI and restart if necessary. 	

2.2.9. Restore Adaptations

Description and Steps	Notes and Status
<p>Restore and adaptations prior to upgrade. If the release is accompanied by Upgrade Notes, refer to the details on adaptation impact.</p>	

2.2.10. Restore Schedules

Description and Steps	Notes and Status
<p>Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available:</p> <p>Individually for each job:</p> <ol style="list-style-type: none"> 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the Scheduling menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, check the Activate check box. <p>Mass modify:</p> <ol style="list-style-type: none"> 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the bulk load sheet. <hr/> <p>Note: Select the Skip next execution if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter.</p> <hr/> <p>Schedules enabled on the CLI. On the primary application node:</p> <ol style="list-style-type: none"> 1. For disabled schedules that were overlapping the maintenance window, enable. Verify disabled schedules: cluster run all schedule list. Record the IP addresses of nodes and scheduled jobs disabled. 2. Enable schedules: cluster run <node IP> schedule enable <job-name> 	

2.2.11. Log Files and Error Checks

Description and Steps	Notes and Status
<p>Inspect the output of the command line interface for upgrade errors. On the primary application node, use the log view command to view any log files indicated in the error messages, for example, run the command if the following message appears:</p> <p>For more information refer to the execution log file with 'log view platform/execute.log'</p> <p>For example, if it is required send all the install log files in the <code>install</code> directory to an SFTP server:</p> <ul style="list-style-type: none"> • log send sftp://x.x.x.x install 	
<p>Log in on the GUI as system level administrator, go to Administration Tools > Transaction and inspect the transactions list for errors.</p>	

3. Single Node Upgrade

3.1. Upgrade a Single Node Cluster Environment with the Delta Bundle

Note:

- While system upgrade takes approximately two hours at a single site, this may vary in accordance with your topology, number of devices and subscribers. Adjust your upgrade maintenance window to allow for your configuration.

The standard **screen** command should be used where indicated. See: *Using the screen command*.

3.1.1. Download Files and Check

Description and Steps	Notes and Status
<p>VOSS files: https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade where XXX is the release number. Download XXX-Delta-Bundle.script file. Transfer the XXX-Delta-Bundle.script file to the media/ folder. Two transfer options: Either using SFTP:</p> <ul style="list-style-type: none">• sftp platform@<unified_node_hostname>• cd media• put <XXX-Delta-Bundle.script> <p>Or using SCP:</p> <ul style="list-style-type: none">• scp <XXX-Delta-Bundle.script> platform@<unified_node_ip_address>:~/media <p>Verify that the .script file copied:</p> <ul style="list-style-type: none">• ls -l media/ <p>Verify that the original .sha256 checksums on the SFTP server match.</p> <ul style="list-style-type: none">• system checksum media/<XXX-Delta-Bundle.script> Checksum: <SHA256>	

3.1.2. Adaptations Check

Description and Steps	Notes and Status
Identify installed adaptations and determine any effect on the upgrade plan. If the release is accompanied by Upgrade Notes, refer to the details.	

3.1.3. Schedules, Transactions and Version Check

Description and Steps	Notes and Status
<p>Turn off any scheduled imports to prevent syncs triggering part way through the upgrade. Two options are available: Individually for each job:</p> <ol style="list-style-type: none"> 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the Scheduling menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, uncheck the Activate check box. <p>Mass modify:</p> <ol style="list-style-type: none"> 1. On the GUI, export scheduled syncs into a bulk load sheet. 2. Modify the schedule settings to de-activate scheduled syncs. 3. Import the sheet. <p>Schedules enabled on the CLI:</p> <ol style="list-style-type: none"> 1. Run schedule list to check if any schedules exist and overlap with the maintenance window. 2. For overlapping schedules, disable. Run schedule disable <job-name>. 	
<p>Check for running imports. Either wait for them to complete or cancel them:</p> <ol style="list-style-type: none"> 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the Transaction menu to view transactions. 3. Filter the Action column: <ol style="list-style-type: none"> a. Choose Status as "Processing" and then choose each Action that starts with "Import", for example, "Import Unity Connection". b. Click Search and confirm there are no results. c. If there are transactions to cancel, select them and click Cancel. 	
<p>Customized ``data/Settings`` If <code>data/Settings</code> instances have been modified, record these or export them as JSON. The modifications can be re-applied or exported JSON instances can be merged following the upgrade. See: Post Template Upgrade Tasks.</p> <p>Version Record the current version information. This is required for upgrade troubleshooting.</p> <ul style="list-style-type: none"> • Log in on the GUI and record the information contained in the About > Extended Version 	

3.1.4. Pre-Upgrade, Security and Health Steps

Description and Steps	Notes and Status
<p>Validate the system health.</p> <p>diag health</p> <p>If there is any sign of the paths below are over 80% full, a clean-up is needed to avoid risk of full logs occurring during upgrade. Clean-up steps are indicated next to the paths:</p> <pre> / (call support if over 80%) /var/log (run: log purge) /opt/platform (remove any unnecessary files from /media directory) /tmp (reboot)</pre> <p>Verify there are no pending Security Updates:</p> <p>security check</p>	
<p>Create a restore point.</p> <p>As part of the rollback procedure, ensure that a suitable restore point is obtained prior to the start of the activity, as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.</p> <p>VOSS cannot guarantee that a restore point can be used to successfully restore VOSS Automate. If you cannot restore the application from a restore point, your only recourse is to reinstall the application.</p> <p>After the restore point has been created, restart.</p> <p>Optional: If a backup is required in addition to the restore point, use the backup add <location-name> and backup create <location-name> commands. For details, refer to the Platform Guide.</p>	

Description and Steps	Notes and Status
<p>Before upgrading, check all services:</p> <p>Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on a fresh node.</p> <ul style="list-style-type: none"> • app status <p>Verify the node is not in the 'recovering' state (<code>stateStr</code> is not RECOVERING)</p> <ul style="list-style-type: none"> • database config 	

3.1.5. Upgrade

Description and Steps	Notes and Status
<p>It is recommended that the upgrade steps are run in a terminal opened with the screen command.</p> <ul style="list-style-type: none"> • screen <p>Run (optionally with command parameters below):</p> <ul style="list-style-type: none"> • app install media/<script_file> <p>From release 19.1.2 and later, the <code>delete-on-success</code> parameter and <code>yes</code> or <code>no</code> value have been added to remove or keep the the script file in the <code>media/</code> directory after successful installation.</p> <p>Note that during the upgrade, phone registration data is cleared. A message will show in the log: <code>Remove phone registration data</code>. This is required so that old values are not displayed, since after the upgrade this information is no longer stored in the resource cache.</p>	

3.1.6. Post-Upgrade, Security and Health Steps

Description and Steps	Notes and Status
<p>Verify the status:</p> <ul style="list-style-type: none"> • diag health 	
<p>If upgrade is successful, the screen session can be closed by typing exit in the screen terminal. If errors occurred, keep the screen terminal open for troubleshooting purposes and contact VOSS support.</p>	
<p>Check for needed security updates.</p> <ul style="list-style-type: none"> • security check <p>If one or more updates are required, complete all the security updates.</p> <ul style="list-style-type: none"> • security update <p>Note: <i>if the system reboots, do not carry out the next manual reboot step.</i> Manual reboot <i>only if needed</i>:</p> <ul style="list-style-type: none"> • system reboot 	

3.1.7. Post Template Upgrade Tasks

Description and Steps	Notes and Status
<p>Customized ``data/Settings`` Merge the previously backed up customized <code>data/Settings</code> with the latest settings on the system by manually adding the differences or exporting the latest settings to JSON, merging the customized changes and importing the JSON.</p> <p>Support for VG400 and VG450 Analogue Gateways Before adding the VG400 or VG450 Gateway, the <code>device/cucm/GatewayType</code> model needs to be imported for each Unified CM.</p> <ol style="list-style-type: none"> 1. Create a Model Type List which includes the <code>device/cucm/GatewayType</code> model. 2. Add the Model Type List to all the required Unified CM Data Syncs. 3. Execute the Data Sync for all the required Unified CMs. <p>Verify the upgrade Log in on the GUI and check the information contained in the About > Version menu. Confirm that versions have upgraded.</p> <ul style="list-style-type: none"> • Release should show 21.2 • Platform Version should show 21.2 <p>If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again.</p>	
<ul style="list-style-type: none"> • Check themes on all roles are set correctly 	

3.1.8. Restore Adaptations

Description and Steps	Notes and Status
<p>Restore and adaptations prior to upgrade. If the release is accompanied by Upgrade Notes, refer to the details on adaptation impact.</p>	

3.1.9. Restore Schedules

Description and Steps	Notes and Status
<p>Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available:</p> <p>Individually for each job:</p> <ol style="list-style-type: none"> 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the Scheduling menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, check the Activate check box. <p>Mass modify:</p> <ol style="list-style-type: none"> 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the bulk load sheet. <hr/> <p>Note: Select the Skip next execution if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter.</p> <hr/> <p>Schedules enabled on the CLI:</p> <ol style="list-style-type: none"> 1. For disabled schedules that were overlapping the maintenance window, enable. Run schedule enable <job-name>. 	

3.1.10. Log Files and Error Checks

Description and Steps	Notes and Status
<p>Inspect the output of the command line interface for upgrade errors.</p> <p>Use the log view command to view any log files indicated in the error messages, for example, run the command if the following message appears:</p> <p>For more information refer to the execution log file with 'log view platform/execute.log'</p> <p>For example, if it is required send all the install log files in the <code>install</code> directory to an SFTP server:</p> <ul style="list-style-type: none"> • log send sftp://x.x.x.x install 	
<p>Log in on the GUI as system level administrator, go to Administration Tools > Transaction and inspect the transactions list for errors.</p>	

Index

A

app
 app template, 2

C

cluster
 cluster primary role application, 11
 cluster primary role database, 11
 cluster provision, 2
 cluster run, 11
 cluster run <IP>, 11
 cluster run all, 11
 cluster run application, 11
 cluster run database, 11
 cluster status, 4, 11
 cluster upgrade, 2, 4, 11

S

screen, 2, 4, 11, 19

V

voss
 voss post-upgrade-migrations, 19
voss export
 voss export group, 2
 voss export type, 2
voss subscriber_data_export, 2