VOSS Automate
Upgrade Guide with ISO and Template

Release 24.1

Sep 12, 2024

Legal Information

DOCUMENT ID: 20240912133405

Contents

1. What's New

1.1. Upgrade Guide with ISO and Template: Release 24.1

- VOSS-1187: Add Visualization Options and Configurable Dashboards to the Automate Portal. See: *VOSS Automate Hardware Specifications*

  Docs added for the new Analytics dashboards in Automate.

- VOSS-1187: Add Visualization Options and Configurable Dashboards to the Automate Portal. See: *Modular Cluster Topology: Upgrade a Multinode Environment with the ISO and Template*

  Docs added for the new Analytics dashboards in Automate.

- VOSS-1187: Add Visualization Options and Configurable Dashboards to the Automate Portal. See: *Modular Cluster Topology: Upgrade a Multinode Environment with the ISO and Template*

  Docs added for the new Analytics dashboards in Automate.

- VOSS-1187: Add Visualization Options and Configurable Dashboards to the Automate Portal. See: *Upgrade a Single Node Cluster Environment with the ISO and Template*

  Docs added for the new Analytics dashboards in Automate.

2. Introduction

Before starting with this upgrade, please read the following notes related to upgrades from earlier versions of the software.

Normal operations will be interrupted during an upgrade. Perform the upgrade in a maintenance window. Refer to the type of upgrade for details on the upgrade duration.

Release 21.4 onwards - Product License Changes

From release 21.4 onwards, VOSS Automate allows for the registration and update of product licenses within the application. A licensing service is installed during installation or upgrade and a license token is associated with the platform on which it is installed.

Release 24.1 onwards - Role changes for managing Microsoft resource accounts

Starting with Automate 24.1, Microsoft requires that you use application registration (app registration) for authentication. If you wish to use basic authentication with service account credentials, please contact VOSS support for assistance. Until Microsoft implements changes to their resource account infrastructure, basic auth is required to create, update, and delete resource accounts. List (import/sync) of resource accounts is supported with app registration authentication in Automate 24.1.

If you wish to manage resource accounts in Automate, you'll need to set up a service account with an additional role assigned, "User Administrator", "Global Administrator", or custom roles that include the "User Management" permission.

See the following references:

- VOSS Automate 24.1 - Microsoft Customers, Upgrade Planning for App Registration
- Create MS Teams Service Account on Microsoft Cloud in the Core Feature Guide

3. Upgrade Planning

3.1. Upgrade and Data Migration

After the upgrade of the system with **app upgrade <file.ISO>** or **cluster upgrade <file.ISO>**, any changes and updates to core model schemas need to be added to the system database. It is recommended that this step is run in a terminal opened with the **screen** command.

This database upgrade is carried out from the Command Line Interface (CLI) by means of **voss upgrade_db**. It is recommended that this step is run in a terminal opened with the **screen** command.

From instructions in the newly upgraded ISO, the schemas of system core models are updated as required and existing data is migrated to these updated model schemas. Schema updates would include updated version numbers and may for example add or remove new model attributes to schemas and add new default data.

Migration instructions from existing model versions to new updated versions are used to create the updated model schemas and update data to be stored in the system database.

In the case of the installation of an updated template, the **app template <template_file>** command will also execute any migration instructions included in the template file to upgrade the database with the updated template data.

3.2. 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

3.3. Unified Node and Modular Cluster Topology Preparation

3.3.1. VOSS Automate Hardware Specifications

Overview

Note: For details around the open source software components used in Automate, see the *Open Source License Usage Guide*.

Virtualized Hardware and Resource Oversubscription

It is recommended that no more than two Unified nodes and one Web Proxy node be run on a physical server (VMware server) and that the disk subsystems are unique for each Unified node.

VOSS Automate virtual machines should maintain a 1:1 ratio between virtual RAM and Disk hardware and physical hardware, in other words:

- 1 GB of virtual RAM (vRAM) must map to 1 GB of physical RAM
- 1 GB of virtual Disk (vDisk) storage must map to 1 GB of physical storage

For virtual CPU (vCPU), hyper-threading is supported.

Unified Node Hardware Specifications

Single-node Cluster (cluster-of-one) Hardware Specification

This section provides the virtual machine specification for a single node cluster deployment topology in VOSS Automate.

Node type	Quantity	VM	Memory	CPU	Disk	Network
Single node cluster	1	>= VMware 5.1	16 GB with 16 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	370 GB partitioned: • 20 GB for OS • 50 GB for application: 10 GB for logs, 40GB for our apps • 50 GB for compressed backups • 250 GB for database 70 GB database disk to be added after upgrade or installation. Refer to the Upgrade Guide with ISO and Template or Installation Guide.	1 Gbit/s minimum

For Memory and CPU, the Resource Allocation Reservation on VMware is indicated in the table. Hyper-threading is supported.

Note:

- From release 24.1, allowance should be made for an additional 70GB database disk to be added after upgrade or installation. This disk will be used for Insights sync.

  Refer to the Upgrade Guide with ISO and Template or Installation Guide and *Steps to add disks in the AWS or MS Azure cloud hosted platform*.

- If memory allocations are customized, ensure that the memory reservation remains equal to the allocated memory in order to prevent possible negative side-effects due to memory reclamation.

For VMware details, refer to the VMware Support topic in the Compatibility Matrix.

The maximum number of users for a single node cluster is 50,000.

Multinode Cluster Hardware Specification

Virtual machine requirements are specified in the table below.

Node type	Quantity	VM	Memory	CPU	Disk	Network
Unified	4 or 6	>= VMware 5.1	32 GB with 32 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	370 GB partitioned: • 20 GB for OS • 50 GB for application: 10 GB for logs, 40GB for our apps • 50 GB for compressed backups • 250 GB for database 70 GB database disk to be added after upgrade or installation. Refer to the Upgrade Guide with ISO and Template or Installation Guide.	1 Gbit/s minimum
WebProxy	2	>= VMware 5.1	4 GB with 4 GB reservation	2 vCPU @ 2 GHz with no reservation	70 GB partitioned: • 20 GB for OS • 50 GB for application	1 Gbit/s minimum

For Memory and CPU, the Resource Allocation Reservation on VMware is indicated in the table. Hyperthreading is supported.

Note:

- From release 24.1, allowance should be made for an additional 70GB database disk to be added after upgrade or installation. This disk will be used for Insights sync.

  Refer to the Upgrade Guide with ISO and Template or Installation Guide and *Steps to add disks in the AWS or MS Azure cloud hosted platform*.

- If memory allocations are customized, ensure that the memory reservation remains equal to the allocated memory in order to prevent possible negative side-effects due to memory reclamation.

The OS disk requirement is fixed and logs are rotated to ensure that 10 GB is sufficient. 40 GB for applications is a generous allocation and does not scale with the number of users.

The Database storage partition is sized to support 250 K users. Database backups are compressed and the partition is sized to ensure that sufficient space available to support backup of 250 GB database.

Note: To change the TRANSACTION_LOG cap size to greater than 10GB at larger providers for operational reasons, for example for diagnostics and a longer transaction replay window, the **voss db_collection_cap TRANSACTION_LOG <10-50GB>** command can be used from the command line.

Refer to Database Commands in the Platform Guide for more details.

The resize operation will impact the usage on the disk size allocated for the database (typically, 250GB is reserved upon installation). Consider a larger database disk size allocation upon installation if a larger cap size is set.

The backup disk should be Thick Provisioned and Eager Zeroed for better performance immediately after installation.

Web Proxies are optional, but if Web Proxies are used, then they form part of the cluster to allow sharing of static data and other content as needed (for example, themes).

To set up the disk requirements, the disk should be set up on the VMware GUI Resources tab where a disk can be created. This task should be done after the OVA import but prior to the boot of the system.

For VMware details, refer to the VMware Support topic in the Compatibility Matrix.

2 Node Cluster Hardware Specification

Virtual machine requirements are specified in the table below.

Node type	Quantity	VM	Memory	CPU	Disk	Network
Unified	= 2	>= VMware 5.1	32 GB with 32 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	370 GB partitioned: • 20 GB for OS • 50 GB for application: 10 GB for logs, 40GB for our apps • 50 GB for compressed backups • 250 GB for database 70 GB database disk to be added after upgrade or installation. Refer to the Upgrade Guide with ISO and Template or Installation Guide.	1 Gbit/s minimum
WebProxy	>= 0	>= VMware 5.1	4 GB with 4 GB reservation	2 vCPU @ 2 GHz with no reservation	70 GB partitioned: • 20 GB for OS • 50 GB for application	1 Gbit/s minimum

For Memory and CPU, the Resource Allocation Reservation on VMware should correspond with these requirements.

Note:

- From release 24.1, allowance should be made for an additional 70GB database disk to be added after upgrade or installation. This disk will be used for Insights sync.

  Refer to the Upgrade Guide with ISO and Template or Installation Guide and *Steps to add disks in the AWS or MS Azure cloud hosted platform*.

- If memory allocations are customized, ensure that the memory reservation remains equal to the allocated memory in order to prevent possible negative side-effects due to memory reclamation.

For VMware details, refer to the VMware Support topic in the Compatibility Matrix.

Modular Cluster Hardware Specifications

Multinode Modular Cluster Hardware Specification

Virtual machine requirements are specified in the table below.

Node type	Quantity	VM	Memory	CPU	Disk	Network
Application	3	>= VMware 5.1	32 GB with 32 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	80 GB partitioned: • 20 GB for OS • 50 GB for application: 10 GB for logs, 40GB for our apps	1 Gbit/s minimum
Database	3	>= VMware 5.1	32 GB with 32 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	380 GB partitioned: • 20 GB for OS • 50 GB for compressed backups • 50 GB for application: – 10 GB for logs – 40GB for our apps • 250 GB for database 70 GB database disk to be added after upgrade or installation. Refer to the Upgrade Guide with ISO and Template or Installation Guide.	1 Gbit/s minimum
WebProxy	2	>= VMware 5.1	4 GB with 4 GB reservation	2 vCPU @ 2 GHz with no reservation	70 GB partitioned: • 20 GB for OS • 50 GB for application	1 Gbit/s minimum

For Memory and CPU, the Resource Allocation Reservation on VMware is indicated in the table. Hyperthreading is supported.

Note:

- From release 24.1, allowance should be made for an additional 250GB database disk to be added after upgrade or installation. This disk will be used for Insights sync.

  Refer to the Upgrade Guide with ISO and Template or Installation Guide and *Steps to add disks in the AWS or MS Azure cloud hosted platform*.

- If memory allocations are customized, ensure that the memory reservation remains equal to the allocated memory in order to prevent possible negative side-effects due to memory reclamation.

The OS disk requirement is fixed and logs are rotated to ensure that 10 GB is sufficient. 40 GB for an applications role node is a generous allocation and the size will not have to be increased with the number of

users.

The Database storage partition is sized to support 250 K users. Database backups are compressed and the partition is sized to ensure that sufficient space is available to support backup of 250 GB database.

Note: To change the TRANSACTION_LOG cap size to greater than 10GB at larger providers for operational reasons, for example for diagnostics, the **voss db_collection_cap TRANSACTION_LOG <10-50GB>** command can be used from the command line.

Refer to Database Commands in the Platform Guide for more details.

The resize operation will impact the usage on the size of the disk allocated for the database (typically, 250GB is reserved upon installation). Consider a larger database disk size allocation upon installation if a larger cap size is set.

The backup disk should be Thick Provisioned and Eager Zeroed for better performance immediately after installation.

Web Proxies are optional, but if Web Proxies are used, then they form part of the cluster to allow sharing of static data and other content as needed (for example, themes).

To set up the disk requirements, the disk should be set up on the VMware GUI Resources tab where a disk can be created. This task should be done after the OVA import but prior to the boot of the system.

For VMware details, refer to the VMware Support topic in the Compatibility Matrix.

Steps to add disks in the AWS or MS Azure cloud hosted platform

The steps below are required to add a disk that provides for the Insights database in release 24.1 - that should then be assigned to the `insights-voss-sync:database` mount point (refer to the final step in the *Upgrade Guide with ISO and Template* for your topology).

1. Create the EBS Volumes for each DB node in the Amazon EC2 console.

   Go to **EC2 > Volumes > Create volume**

   For **Volume settings**, enter:

   - Volume type: Provisioned IOPS SSD (io2)
   - Size (GiB): 70GB
   - IOPS: 750

   For **Availability Zone**:

   - Create 3 volumes in each of the zones (for example: us-east-1a, us-east-1b, us-east-1c)

2. Attach the newly created volumes to each of the database nodes.

   Go to **EC2 > Volumes > volume_id > Attach volume**

   - **Instance**: Select the database instance within the same corresponding az
   - **Device Name**: `/dev/sde` (This will display as `xvde` in drives list)

1. In the MS Azure portal, search for Virtual Machines
   - Select each of the database nodes
   - Select **Disk** under **Properties**
2. Click “Create and attach a new disk”

- **LUN**: Next avaiable
- **Disk Name**: Label according to your recommended naming convention
- **Storage Type**: Premium SSD LRS
- **Size**: 70GB
- **Encryption**: Set according to your requirements
- **Host Caching**: Read/Write

4. Multinode Upgrade

4.1. Unified Node Topology: Upgrade a Multinode Environment with the ISO and Template

Important:

- Before upgrading to release 24.1:

  Install `EKB-21455-21.4.0_patch.script` first. Refer to `MOP-EKB-21455-21.4.0_patch.pdf`.

  - **Server Name**: https://voss.portalshape.com
  - **Path**: **Downloads > VOSS Automate > 24.1 > Upgrade > ISO**
  - **MOP**: MOP-EKB-21455-21.4.0_patch.pdf
  - **Patch File**: EKB-21455-21.4.0_patch.script

- Before upgrading to release 24.1, ensure that:

  - an additional 70 GB disk is available for the Insights database
  - all unified nodes memory allocation is 32 GB with 32 GB reservation

  See the Adding Hard Disk Space topic in the Platform Guide and VOSS Automate Hardware Specifications in the Architecture and Hardware Specification Guide.

  This disk is needed to assign to the `insights-voss-sync:database` mount point. See: *Mount the Insights disk (outside, after Maintenance Window)*.

- Before upgrading to release 24.1, ensure that sufficient time is allocated to the maintenance window. This may vary in accordance with your topology, number of devices and subscribers.

  The information below serves as a guideline VOSS support can be contacted if further guidance is required:

  - Cluster upgrade: 4h
  - Template install: 2.5h
  - For a 500K Data User system (13Mil RESOURCE documents), the expected `upgrade_db` step is about 12h.
  - For a 160K Data User system (2.5Mil RESOURCE documents), the expected `upgrade_db` step is about 2.5h.

  You can follow the progress on the Admin Portal transaction list.

- Tasks that are marked **Prior to Maintenance Window** can be completed a few days prior to the scheduled maintenance window so that VOSS support can be contacted if needed and in order to allow for reduce down time.

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

4.1.1. Download Files and Check (Prior to Maintenance Window)

Note: Ensure that the `.iso` file is available on *all* nodes.

Description and Steps	Notes and Status
VOSS files: **https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade** Download `.iso` and `.template` files, where XXX matches the release. • Transfer the `.iso` file to the `media/` folder of all nodes. • Transfer the `.template` file to the `media/` folder of the primary node. Two transfer options: Either using SFTP: • **sftp platform@<unified_node_hostname>** • **cd media** • **put <upgrade_iso_file>** • **put <upgrade_template_file>** Or using SCP: • **scp <upgrade_iso_file> platform@<unified_node_ip_address>:~/media** • **scp <upgrade_template_file> platform@<unified_node_ip_address>:~/media** Verify that the `.iso` image and `.template` file copied: • **ls -l media/** Verify that the original `.sha256` checksums on the Download site server match. • **system checksum media/<upgrade_iso_file>** `Checksum: <SHA256>` • **system checksum media/<upgrade_template_file>** `Checksum: <SHA256>`	

4.1.2. Version Check (Prior to Maintenance Window)

Description and Steps	Notes and Status
Customized ``data/Settings`` If `data/Settings` 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 (Maintenance Window)*. **Version** Record the current version information. This is required for upgrade troubleshooting. • Log in on the Admin Portal and record the information contained in the menu: **About > Version**	

4.1.3. Security and Health Check Steps (Maintenance Window)

Description and Steps	Notes and Status

Choose an option:
• **If you're upgrading from: [21.4-PB4, 21.4-PB5]**
Place the system in maintenance mode to suspend any scheduled transactions. Scheduled transactions that are in progress will be allowed to complete, or otherwise, cancel data sync transactions that are in progress on the GUI. Refer to the Core Feature Guide. For details, refer to the System Maintenance Mode topic in the Platform Guide.
On an application node of the system, run:
`cluster maintenance-mode start`
You can verify the maintenance mode status with:
`cluster maintenance-mode status`
• **If you're upgrading from: [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]**
Turn off any scheduled imports to prevent syncs triggering part way through the upgrade.
--- 	
Note: Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu available on the available on the `MVS-DataSync-Dashboard`.
--- 	
Two options are available:
Individually for each job:
1. Log in on the Admin Portal 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.
Mass modify:
1. On the Admin Portal, export scheduled syncs into a bulk load sheet.
2. Modify the schedule settings to de-activate scheduled syncs.
3. Import the sheet.
Schedules enabled on the CLI:
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>**.
Verify that the primary node is the active primary node at the time of upgrade.
database config
Ensure that the node on which the installation will be initiated has the `stateStr` parameter set to **PRIMARY** and has the **highest** `priority` **number** (highest priority number could vary depending on cluster layout).
Example output
`<ip address>:27020:`
`  priority: <number>`
`  stateStr: PRIMARY`
`  storageEngine: WiredTiger`	

Description and Steps	Notes and Status

The following step is needed if own private certificate and generated SAN certificates are required and the `web cert gen_csr` command was run. For details, refer to the Web Certificate Setup Options topic in the Platform Guide.
The steps below are needed to check if a CSR private key exists but no associated signed certificate is available.
Request VOSS support to run on the CLI as `root` user, the following command:
`for LST in /opt/platform/apps/nginx/config/csr/*;`
`do openssl x509 -in $LST -text -noout >/dev/null`
`2>&1 && SIGNED="$LST"; done`
 	
`echo $SIGNED`
If the `echo $SIGNED` command output is blank, back up the `csr/` directory with for example the following command:
`mv /opt/platform/apps/nginx/config/csr/ /opt/platform/apps/nginx/config/csrbackup`	

Description and Steps	Notes and Status

Validate the system health. Carry out the following:
• **system mount** - mount upgrade ISO.
• **app install check_cluster** - install the new version of the **cluster check** command. For details, refer to the "Cluster Check" topic in the Platform Guide.
• **cluster check** - inspect the output of this command for warnings and errors. You can also use **cluster check verbose** to see more details, for example, `avx` enabled. While warnings will not prevent an upgrade, it is advisable that these be resolved prior to upgrading where possible. Some warnings may be resolved by upgrading. For troubleshooting and resolutions, also refer to the *Health Checks for Cluster Installations Guide* and *Platform Guide*.
If there is any sign of the paths below are over 80% full, a clean-up is needed, for example to avoid risk of full logs occurring during upgrade. Clean-up steps are indicated next to the paths:
`/ (call support if over 80%)`
`/var/log (run: log purge)`
`/opt/platform (remove any unnecessary files from /media directory)`
`/tmp (reboot)`
On the Primary Unified Node, verify there are no pending Security Updates on any of the nodes.
 	
Note: If you run **cluster status** after installing the new version of **cluster check**, any error message regarding a failed command can be ignored. This error message will not show after upgrade.	

4.1.4. Pre-Upgrade Steps (Maintenance Window)

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. 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*.	

Description and Steps	Notes and Status

After restore point creation and before upgrading: validate system health and check all services, nodes and weights for the cluster:
• **cluster run application cluster list**
Make sure all application nodes show 4 or 6 nodes.
• **cluster check** - inspect the output of this command, for warnings and errors. You can also use **cluster check verbose** to see more details.
– Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh unified nodes.
– Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster. Example output:
`172.29.21.240:`
`  weight: 80`
`172.29.21.241:`
`  weight: 70`
`172.29.21.243:`
`  weight: 60`
`172.29.21.244:`
`  weight: 50`
– Verify the primary node in the primary site and ensure no nodes are in the 'recovering' state (`stateStr` is not `RECOVERING`). On the primary node:	

4.1.5. Upgrade (Maintenance Window)

Note:

- By default, the cluster upgrade is carried out in parallel on all nodes and without any backup in order to provide a fast upgrade.
- For systems *upgrading to 24.1 from 21.4.0 - 21.4-PB5*:
  - The VOSS platform maintenance mode will be started automatically when the **cluster upgrade** command is run. This prevents any new occurrences of scheduled transactions, including the 24.1 database syncs associated with **insights sync**. For details on **insights sync**, see the *Insights Analytics* topic in the Platform Guide.
  - The **cluster maintenance-mode stop** command must however be run manually after the maintenance window of the upgrade: *End of the Maintenance Window and Restoring Schedules*.

For details on the VOSS platform maintenance mode, see the *Maintenance Mode* topic in the Platform Guide.

Description and Steps	Notes and Status

It is recommended that the upgrade steps are run in a terminal opened with the **screen** command.
Verify that the ISO has been uploaded to the `media/` directory on each node. This will speed up the upgrade time.
On the primary unified node:
• **screen**
• **cluster upgrade media/<upgrade_iso_file>**
Note: If the system reboots, do not carry out the next manual reboot step.
Manual reboot *only if needed*:
• **cluster run notme system reboot**
If node messages: `<node name> failed with timeout` are displayed, these can be ignored.
• **system reboot**
Since all services will be stopped, this takes some time.
Close **screen**: `Ctrl-a \`
Log in on the primary database node and run **cluster run database app status**. If the report shows `insights-voss-sync:realtime stopped` on some database nodes, request assistance with root access on the system CLI from VOSS support in order to carry out the following on the primary database node:
1. Run the command:
`/opt/platform/mags/insights-voss-sync-mag-script install database`
This should return: `Configured Postgres secrets`.
2. Verify that the database nodes now all have the correct mongo info:
`cluster run database diag config app insights-voss-sync /mongo`
All nodes should have the password/port/user shown as below:
`mongo:`
`password: ********`
`port: 27020`
`user: insights-platform`
3. Restart the `insights-voss-sync:real-time` service on all database nodes:
`cluster run database app start insights-voss-sync:real-time`	

All unused docker images except `selfservice` and `voss_ubuntu` images will be removed from the system at this stage.

4.1.6. Post-Upgrade, Security and Health Steps (Maintenance Window)

Description and Steps	Notes and Status

On each unified node, assign the `insights-voss-sync:database` mount point to the drive added for the Insights database prior to upgrade.
For example, if `drives list` shows the added disk as:
`Unused disks:`
`sde`
then run the command
`drives add sde insights-voss-sync:database`
on each unified node where the drive has been added.
Output is typically (the message below can be ignored on release 24.1:
`WARNING: Failed to connect to lvmetad. Falling back to device scanning.`
)	

On the primary database node, verify the 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** For a cloud deployment (MS Azure / AWS), also refer to the steps below.	

Check for needed security updates. On the primary node, run:
• **cluster run all security check**
If one or more updates are required for any node, run on the primary Unified node:
• **cluster run all security update**
If upgrading a cloud deployment (MS Azure / AWS), run **cluster check**. If an error shows at each node:
`grub-pc: package in an undesired state`
then request assistance with root access on the system CLI from VOSS Support in order to run the command on each node:
`dpkg --configure -a`
A text user interface opens and you will be prompted:
– "GRUB install devices:"- Do *not* select any device. Press <Tab> to highlight <Ok> and press <Enter>.
– At "Continuing without installing GRUB?", press <Yes>
– Exit root user, run **cluster check** again and verify the error does not show.
Note: *if the system reboots, do not carry out the next manual reboot step*.
Manual reboot *only if needed*:
• **cluster run notme system reboot**
If node messages: `<node name> failed with timeout` are displayed, these can be ignored.
• **system reboot**
Since all services will be stopped, this takes some time.	

To remove a mount directory `media/<iso_file basename>` on nodes that may have remained after for example an upgrade, run: **cluster run all app cleanup**	
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.	

4.1.7. Database Schema Upgrade (Maintenance Window)

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. On the primary unified node: • **screen** • **voss upgrade_db** Check cluster status • **cluster check**	

4.1.8. Template Upgrade (Maintenance Window)

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. On the primary unified node: • **screen** • **app template media/<VOSS Automate.template>**	

The following message appears:

```
Running the DB-query to find the current environment's
existing solution deployment config...
```

- Python functions are deployed
- System artifacts are imported.

Note: In order to carry out fewer upgrade steps, the updates of instances of some models are skipped in the cases where:

- `data/CallManager` instance does not exist as instance in `data/NetworkDeviceList`
- `data/CallManager` instance exists, but `data/NetworkDeviceList` is empty
- Call Manager AXL Generic Driver and Call Manager Control Center Services match the `data/CallManager` IP

The template upgrade automatically detects the deployment mode: “Enterprise” or “Provider”

A message displays according to the selected deployment type. Check for one of the messages below:

```
Importing EnterpriseOverlay.json

Importing ProviderOverlay.json ...
```

The template install automatically restarts necessary applications. If a cluster is detected, the installation propagates changes throughout the cluster.

Description and Steps	Notes and Status

Review the output from the **app template** command and confirm that the upgrade message appears:
`Deployment summary of PREVIOUS template solution`
`(i.e. BEFORE upgrade):`
`------------------------------------------------`
 	
`Product: [PRODUCT]`
`Version: [PREVIOUS PRODUCT RELEASE]`
`Iteration-version: [PREVIOUS ITERATION]`
`Platform-version: [PREVIOUS PLATFORM VERSION]`
This is followed by updated product and version details:
`Deployment summary of UPDATED template solution`
`(i.e. current values after installation):`
`------------------------------------------------`
 	
`Product: [PRODUCT]`
`Version: [UPDATED PRODUCT RELEASE]`
`Iteration-version: [UPDATED ITERATION]`
`Platform-version: [UPDATED PLATFORM VERSION]`	

Description and Steps	Notes and Status
• If no errors are indicated, create a restore point. This restore point can be used if post-upgrade patches that may be required, fail. 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.	

For an unsupported upgrade path, the install script stops with the message:
`Upgrade failed due to unsupported upgrade path.`
`Please log in as sysadmin`
`and see Transaction logs for more detail.`
You can roll back as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.	

If there are errors for another reason, the install script stops with a failure message listing the problem. Contact VOSS support.	
Verify the `extra_functions` have the *same checksum* across the cluster. • **cluster run application voss get_extra_functions_version -c**	
Post upgrade migrations: On a single node of a cluster, run: • **voss post-upgrade-migrations**	

Data migrations that are not critical to system operation can have significant execution time at scale. These need to be performed after the primary upgrade, allowing the migration to proceed whilst the system is in use - thereby limiting upgrade windows.

A transaction is queued on VOSS Automate and its progress is displayed as it executes.

Description and Steps	Notes and Status
Check cluster status and health • **cluster status**	

4.1.9. Post Template Upgrade Tasks (Maintenance Window)

Description and Steps	Notes and Status
Verify the upgrade Log in on the Admin Portal and check the information contained in the **About > Version** menu. Confirm that versions have upgraded. • **Release** should show `XXX` • **Platform Version** should show `XXX` where `XXX` corresponds with the release number of the upgrade.	
• Check themes on all roles are set correctly	
• For configurations that make use of the Northbound Billing Integration (NBI), please check the service status of NBI and restart if necessary.	

4.1.10. Log Files and Error Checks (Maintenance Window)

Description and Steps	Notes and Status
Inspect the output of the command line interface for upgrade errors, for example `File import failed!` or `Failed to execute command`. 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: `For more information refer to the execution log file with 'log view platform/execute.log'` For example, if it is required send all the install log files in the `install` directory to an SFTP server: • **log send sftp://x.x.x.x install**	
Log in on the Admin Portal as system level administrator, go to **Administration Tools > Transaction** and inspect the transactions list for errors.	

4.1.11. End of the Maintenance Window and Restoring Schedules

Description and Steps	Notes and Status
On the CLI: Run the **cluster maintenance-mode stop** command to end the VOSS maintenance mode when upgrading to 24.1 from 21.4 or 21.4.-PBx. This will allow scheduled data sync transactions to resume, including **insights sync** operations added in 24.1. For details on the VOSS platform maintenance mode, see the *Maintenance Mode* topic in the Platform Guide. • **If you're upgrading from: [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]** Restore Schedules --- **Note:** Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu available on the available on the `MVS-DataSync-Dashboard`. --- Re-enable scheduled imports if any were disabled prior to the upgrade. Individually for each job: 1. Log in on the Admin Portal 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. Mass modify: 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the sheet. --- **Note:** Select the **Skip next execution** option if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter. --- Schedules enabled on the CLI: For disabled schedules that were overlapping the maintenance window, enable. Run **schedule enable <job-name>**.	

4.1.12. Licensing (outside, after Maintenance Window)

Description and Steps	Notes and Status
From release 21.4 onwards, the deployment needs to be licensed. After installation, a 7-day grace period is available to license the product. Since license processing is only scheduled every hour, if you wish to license immediately, first run **voss check-license** from the primary unified node CLI. 1. Obtain the required license token from VOSS. 2. Steps for GUI and CLI: a. To license through the GUI, follow steps indicated in Product License Management in the Core Feature Guide. b. To license through the CLI, follow steps indicated in Product Licensing in the Platform Guide.	

4.1.13. Mount the Insights disk (outside, after Maintenance Window)

Description and Steps	Notes and Status

On each unified node, assign the `insights-voss-sync:database` mount point to the drive added for the Insights database prior to upgrade.
For example, if `drives list` shows the added disk as:
`Unused disks:`
`sde`
then run the command
`drives add sde insights-voss-sync:database`
on each unified node where the drive has been added.
Sample output (the message below can be ignored on release 24.1:
`WARNING: Failed to connect to lvmetad. Falling back to device scanning.`)
`$ drives add sde insights-voss-sync:database`
`Configuration setting "devices/scan_lvs" unknown.`
`Configuration setting "devices/allow_mixed_block_sizes" unknown.`
`WARNING: Failed to connect to lvmetad. Falling back to device scanning.`
`71ad98e0-7622-49ad-9fg9-db04055e82bc`
`Application insights-voss-sync processes stopped.`
`Migrating data to new drive - this can take several minutes`
`Data migration complete - reassigning drive`
`Checking that /dev/sde1 is mounted`
`Checking that /dev/dm-0 is mounted`
`/opt/platform/apps/mongodb/dbroot`
`Checking that /dev/sdc1 is mounted`
`/backups`
`Application services:firewall processes stopped.`
`Reconfiguring applications...`
`Application insights-voss-sync processes started.`	

4.2. Modular Cluster Topology: Upgrade a Multinode Environment with the ISO and Template

Important:

- When upgrading from an existing Modular Cluster Topology that was available since VOSS Automate 21.1, use the steps listed here.
- Before upgrading to release 24.1:

  Install `EKB-21455-21.4.0_patch.script` first. Refer to `MOP-EKB-21455-21.4.0_patch.pdf`.

  - **Server Name**: https://voss.portalshape.com
  - **Path**: **Downloads > VOSS Automate > 24.1 > Upgrade > ISO**

  - **MOP**: MOP-EKB-21455-21.4.0_patch.pdf
  - **Patch File**: EKB-21455-21.4.0_patch.script
- Before upgrading to release 24.1, ensure that:
  - an additional 70 GB disk is available for the Insights database
  - all application and database nodes memory allocation is 32 GB with 32 GB reservation

  See the Adding Hard Disk Space topic in the Platform Guide and VOSS Automate Hardware Specifications in the Architecture and Hardware Specification Guide.

  This disk is needed to assign to the `insights-voss-sync:database` mount point. See: *Mount the Insights disk (outside, after Maintenance Window)*.
- Before upgrading to release 24.1, ensure that sufficient time is allocated to the maintenance window. This may vary in accordance with your topology, number of devices and subscribers.

  The information below serves as a guideline VOSS support can be contacted if further guidance is required:
  - Cluster upgrade: 4h
  - Template install: 2.5h
  - For a 500K Data User system (13Mil RESOURCE documents), the expected `upgrade_db` step is about 12h.
  - For a 160K Data User system (2.5Mil RESOURCE documents), the expected `upgrade_db` step is about 2.5h.

  You can follow the progress on the Admin Portal transaction list.
- Tasks that are marked **Prior to Maintenance Window** can be completed a few days prior to the scheduled maintenance window so that VOSS support can be contacted if needed and in order to allow for reduce down time.

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

Primary database and application node in a Modular Cluster Topology

- Verify the *primary application node* (UN2) with the **cluster primary role application** command run on the node. The output should be *true*, for example:

```
platform@UN2:~$ cluster primary role application
is_primary: true
```

- Verify the *primary database node* (UN1) with the **cluster primary role database** command run on the node. The output should be *true*, for example:

```
platform@UN1:~$ cluster primary role database
is_primary: true
```

4.2.1. Download Files and Check (Prior to Maintenance Window)

Note: Ensure that the `.iso` file is available on *all* nodes.

Description and Steps	Notes and Status
VOSS files: **https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade** Download `.iso` and `.template` files, where XXX is the release number. • Transfer the `.iso` file to the `media/` folder of the all nodes. • Transfer the `.template` file to the `media/` folder of the primary application node. Two transfer options: Either using SFTP: • **sftp platform@<unified_node_hostname>** • **cd media** • **put <upgrade_iso_file>** • **put <upgrade_template_file>** Or using SCP: • **scp <upgrade_iso_file> platform@<unified_node_ip_address>:~/media** • **scp <upgrade_template_file> platform@<unified_node_ip_address>:~/media** Verify that the `.iso` image and `.template` file copied: • **ls -l media/** Verify that the original `.sha256` checksums on the Download site match. • primary database node: **system checksum media/<upgrade_iso_file>** `Checksum: <SHA256>` • primary application node: **system checksum media/<upgrade_template_file>** `Checksum: <SHA256>`	

4.2.2. Version Check (Prior to Maintenance Window)

Description and Steps	Notes and Status
Version Record the current version information. This is required for upgrade troubleshooting. • Log in on the Admin Portal and record the information contained in the menu: **About > Version**	

4.2.3. Security and Health Check Steps (Prior to Maintenance Window)

Description and Steps	Notes and Status

Choose an option:
• **If you're upgrading from: [21.4-PB4, 21.4-PB5]**
Place the system in maintenance mode to suspend any scheduled transactions. Scheduled transactions that are in progress will be allowed to complete, or otherwise, cancel data sync transactions that are in progress on the GUI. Refer to the Core Feature Guide. For details, refer to the System Maintenance Mode topic in the Platform Guide.
On an application node of the system, run:
`cluster maintenance-mode start`
You can verify the maintenance mode status with:
`cluster maintenance-mode status`
• **If you're upgrading from: [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]**
Turn off any scheduled imports to prevent syncs triggering part way through the upgrade.
--- 	
Note: Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu available on the available on the `MVS-DataSync-Dashboard`.
--- 	
Two options are available:
Individually for each job:
1. Log in on the Admin Portal 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.
Mass modify:
1. On the Admin Portal, export scheduled syncs into a bulk load sheet.
2. Modify the schedule settings to de-activate scheduled syncs.
3. Import the sheet.
Schedules enabled on the CLI:
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>**.
Verify that the primary database node is the active primary node at the time of upgrade.
database config
Ensure that the node on which the installation will be initiated has the `stateStr` parameter set to **PRIMARY** and has the **highest** `priority` **number** (highest priority number could vary depending on cluster layout).
Example output
`<ip address>:27020:`
`  priority: <number>`
`  stateStr: PRIMARY`
`  storageEngine: WiredTiger`	

Description and Steps	Notes and Status

The following step is needed if own private certificate and generated SAN certificates are required and the `web cert gen_csr` command was run. For details, refer to the Web Certificate Setup Options topic in the Platform Guide.
The steps below are needed to check if a CSR private key exists but no associated signed certificate is available.
Request VOSS support to run on the CLI as `root` user, the following command:
`for LST in /opt/platform/apps/nginx/config/csr/*;`
`do openssl x509 -in $LST -text -noout >/dev/null`
`2>&1 && SIGNED="$LST"; done`
 	
`echo $SIGNED`
If the `echo $SIGNED` command output is blank, back up the `csr/` directory with for example the following command:
`mv /opt/platform/apps/nginx/config/csr/ /opt/platform/apps/nginx/config/csrbackup`	

Description and Steps	Notes and Status

Validate the system health. Carry out the following:
• **system mount** - mount upgrade ISO.
• **app install check_cluster** - install the new version of the **cluster check** command. For details, refer to the "Cluster Check" topic in the Platform Guide.
• **cluster check** - inspect the output of this command for warnings and errors. You can also use **cluster check verbose** to see more details, for example, `avx` enabled. While warnings will not prevent an upgrade, it is advisable that these be resolved prior to upgrading where possible. Some warnings may be resolved by upgrading. For troubleshooting and resolutions, also refer to the *Health Checks for Cluster Installations Guide* and *Platform Guide*.
If there is any sign of the paths below are over 80% full, a clean-up is needed, for example to avoid risk of full logs occurring during upgrade. Clean-up steps are indicated next to the paths:
`/ (call support if over 80%)`
`/var/log (run: log purge)`
`/opt/platform (remove any unnecessary files from /media directory)`
`/tmp (reboot)`
On the Primary Unified Node, verify there are no pending Security Updates on any of the nodes.
 	
Note: If you run **cluster status** after installing the new version of **cluster check**, any error message regarding a failed command can be ignored. This error message will not show after upgrade.	

4.2.4. Pre-Upgrade Steps (Maintenance Window)

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. Optional: If a backup is also required - on the primary database node, use the **backup add <location-name>** and **backup create <location-name>** commands. For details, refer to the *Platform Guide*.	

Description and Steps	Notes and Status

After restore point creation and before upgrading: validate system health and check all services, nodes and weights for the cluster:
• **cluster run application cluster list**
Make sure all application nodes show.
• **cluster check** - inspect the output of this command, for warnings and errors. You can also use **cluster check verbose** to see more details.
– Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh database nodes.
– Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster. Example output:
`172.29.21.240:`
`  weight: 80`
`172.29.21.241:`
`  weight: 70`
`172.29.21.243:`
`  weight: 60`
`172.29.21.244:`
`  weight: 50`
– Verify the primary node in the primary site and ensure no nodes are in the 'recovering' state (`stateStr` is not `RECOVERING`). On the primary node:
On the primary application node, verify there are no pending Security Updates on any of the nodes:
• **cluster run all security check**	

4.2.5. Upgrade (Maintenance Window)

Note:

- By default, the cluster upgrade is carried out in parallel on all nodes and without any backup in order to provide a fast upgrade.
- For systems *upgrading to 24.1 from 21.4.0 - 21.4-PB5*:
  - The VOSS platform maintenance mode will be started automatically when the **cluster upgrade** command is run. This prevents any new occurrences of scheduled transactions, including the 24.1 database syncs associated with **insights sync**. For details on **insights sync**, see the *Insights Analytics* topic in the Platform Guide.

  - The **cluster maintenance-mode stop** command must however be run manually after the maintenance window of the upgrade: *End of the Maintenance Window and Restoring Schedules*.

For details on the VOSS platform maintenance mode, see the *Maintenance Mode* topic in the Platform Guide.

Description and Steps	Notes and Status

It is recommended that the upgrade steps are run in a terminal opened with the **screen** command.
Verify that the ISO has been uploaded to the `media/` directory on each node. This will speed up the upgrade time.
On the primary database node:
• **screen**
• **cluster upgrade media/<upgrade_iso_file>**
Close **screen**: `Ctrl-a \`
Log in on the primary database node and run **cluster run database app status**. If the report shows `insights-voss-sync:realtime stopped` on some database nodes, request assistance with root access on the system CLI from VOSS support in order to carry out the following on the primary database node:
1. Run the command: `/opt/platform/mags/insights-voss-sync-mag-script install database` This should return: `Configured Postgres secrets`.
2. Verify that the database nodes now all have the correct mongo info: `cluster run database diag config app insights-voss-sync /mongo` All nodes should have the password/port/user shown as below:
`mongo:`
`  password: ********`
`  port: 27020`
`  user: insights-platform`
3. Restart the `insights-voss-sync:real-time` service on all database nodes: `cluster run database app start insights-voss-sync:real-time`	

All unused docker images except `selfservice` and `voss_ubuntu` images will be removed from the system at this stage.

4.2.6. Post-Upgrade and Health Steps (Maintenance Window)

Description and Steps	Notes and Status
On the primary database node, verify the 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** For a cloud deployment (MS Azure / AWS), also refer to the steps below.	
To remove a mount directory `media/<iso_file basename>` on nodes that may have remained after for example an upgrade, run: **cluster run all app cleanup** on the primary database node.	

Check for needed security updates. On the primary application node, run:
• **cluster run all security check**
If one or more updates are required for any node, run on the primary application node:
• **cluster run all security update**
If upgrading a cloud deployment (MS Azure / AWS), run **cluster check**. If an error shows at each node:
`grub-pc: package in an undesired state`
then request assistance with root access on the system CLI from VOSS Support in order to run the command on each node:
`dpkg --configure -a`
A text user interface opens and you will be prompted:
– "GRUB install devices:"- Do *not* select any device. Press <Tab> to highlight <Ok> and press <Enter>.
– At "Continuing without installing GRUB?", press <Yes>
– Exit root user, run **cluster check** again and verify the error does not show.
Note: *if the system reboots, do not carry out the next manual reboot step*.
Manual reboot *only if needed*:
• **cluster run notme system reboot**
If node messages: `<node name> failed with timeout` are displayed, these can be ignored.
• **system reboot**
Since all services will be stopped, this takes some time.	

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.	

4.2.7. Database Schema Upgrade (Maintenance Window)

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. On the primary application node: • **screen** • **voss upgrade_db** Check cluster status • **cluster check**	

4.2.8. Template Upgrade (Maintenance Window)

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. On the primary application node: • **screen** • **app template media/<VOSS Automate.template>**	

The following message appears:

```
Running the DB-query to find the current environment's
existing solution deployment config...
```

- Python functions are deployed
- System artifacts are imported.

Note: In order to carry out fewer upgrade steps, the updates of instances of some models are skipped in the cases where:

- `data/CallManager` instance does not exist as instance in `data/NetworkDeviceList`
- `data/CallManager` instance exists, but `data/NetworkDeviceList` is empty
- Call Manager AXL Generic Driver and Call Manager Control Center Services match the `data/CallManager` IP

The template upgrade automatically detects the deployment mode: “Enterprise” or “Provider”. A message displays according to the selected deployment type. Check for one of the messages below:

```
Importing EnterpriseOverlay.json

Importing ProviderOverlay.json ...
```

The template install automatically restarts necessary applications. If a cluster is detected, the installation propagates changes throughout the cluster.

Description and Steps	Notes and Status

Review the output from the **app template** command and confirm that the upgrade message appears:
`Deployment summary of PREVIOUS template solution (i.e. BEFORE upgrade):`
`---`
`Product: [PRODUCT]`
`Version: [PREVIOUS PRODUCT RELEASE]`
`Iteration-version: [PREVIOUS ITERATION]`
`Platform-version: [PREVIOUS PLATFORM VERSION]`
This is followed by updated product and version details:
`Deployment summary of UPDATED template solution (i.e. current values after installation):`
`---`
`Product: [PRODUCT]`
`Version: [UPDATED PRODUCT RELEASE]`
`Iteration-version: [UPDATED ITERATION]`
`Platform-version: [UPDATED PLATFORM VERSION]`	

Description and Steps	Notes and Status
• If no errors are indicated, create a restore point. 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.	

For an unsupported upgrade path, the install script stops with the message:
`Upgrade failed due to unsupported upgrade path.`
`Please log in as sysadmin`
`and see Transaction logs for more detail.`
You can roll back as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.	

If there are errors for another reason, the install script stops with a failure message listing the problem. Contact VOSS support.	
On the primary application node, verify the `extra_functions` have the *same checksum* across the cluster. • **cluster run application voss get_extra_functions_version -c**	
Post upgrade migrations: On a single application node of a cluster, run: • **voss post-upgrade-migrations**	

Data migrations that are not critical to system operation can have significant execution time at scale. These need to be performed after the primary upgrade, allowing the migration to proceed whilst the system is in use - thereby limiting upgrade windows.

A transaction is queued on VOSS Automate and its progress is displayed as it executes.

Description and Steps	Notes and Status
Check cluster status and health • on the primary database node: • **cluster status**	

4.2.9. Post Template Upgrade Tasks (Maintenance Window)

Description and Steps	Notes and Status
Verify the upgrade Log in on the Admin Portal and check the information contained in the **About > Version** menu. Confirm that versions have upgraded. • **Release** should show `XXX` • **Platform Version** should show `XXX` where `XXX` corresponds with the release number of the upgrade.	
• Check themes on all roles are set correctly	
• For configurations that make use of the Northbound Billing Integration (NBI), please check the service status of NBI and restart if necessary.	

4.2.10. Log Files and Error Checks (Maintenance Window)

Description and Steps	Notes and Status
Inspect the output of the command line interface for upgrade errors, for example `File import failed!` or `Failed to execute command`. 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: `For more information refer to the execution log file with 'log view platform/execute.log'` For example, if it is required send all the install log files in the `install` directory to an SFTP server: • **log send sftp://x.x.x.x install**	
Log in on the Admin Portal as system level administrator, go to **Administration Tools > Transaction** and inspect the transactions list for errors.	

4.2.11. End of the Maintenance Window and Restoring Schedules

Description and Steps	Notes and Status
On the CLI: Run the **cluster maintenance-mode stop** command to end the VOSS maintenance mode when upgrading to 24.1 from 21.4 or 21.4.-PBx. This will allow scheduled data sync transactions to resume, including **insights sync** operations added in 24.1. For details on the VOSS platform maintenance mode, see the *Maintenance Mode* topic in the Platform Guide. • **If you're upgrading from: [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]** Restore Schedules --- **Note:** Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu available on the available on the `MVS-DataSync-Dashboard`. --- Re-enable scheduled imports if any were disabled prior to the upgrade. Individually for each job: 1. Log in on the Admin Portal 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. Mass modify: 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the sheet. --- **Note:** Select the **Skip next execution** option if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter. --- Schedules enabled on the CLI: For disabled schedules that were overlapping the maintenance window, enable. Run **schedule enable <job-name>**.	

4.2.12. Licensing (outside, after Maintenance Window)

Description and Steps	Notes and Status
From release 21.4 onwards, the deployment needs to be licensed. After installation, a 7-day grace period is available to license the product. Since license processing is only scheduled every hour, if you wish to license immediately, first run **voss check-license** from the primary application node CLI. 1. Obtain the required license token from VOSS. 2. Steps for GUI and CLI: a. To license through the GUI, follow steps indicated in Product License Management in the Core Feature Guide. b. To license through the CLI, follow steps indicated in Product Licensing in the Platform Guide.	

4.2.13. Mount the Insights disk (outside, after Maintenance Window)

Description and Steps	Notes and Status

On each database node, assign the `insights-voss-sync:database` mount point to the drive added for the Insights database prior to upgrade.
For example, if `drives list` shows the added disk as:
`Unused disks:`
`sde`
then run the command
`drives add sde insights-voss-sync:database`
on each unified node where the drive has been added.
Sample output (the message below can be ignored on release 24.1:
`WARNING: Failed to connect to lvmetad. Falling back to device scanning.`)
`$ drives add sde insights-voss-sync:database`
`Configuration setting "devices/scan_lvs" unknown.`
`Configuration setting "devices/allow_mixed_block_sizes" unknown.`
`WARNING: Failed to connect to lvmetad. Falling back to device scanning.`
`71ad98e0-7622-49ad-9fg9-db04055e82bc`
`Application insights-voss-sync processes stopped.`
`Migrating data to new drive - this can take several minutes`
`Data migration complete - reassigning drive`
`Checking that /dev/sde1 is mounted`
`Checking that /dev/dm-0 is mounted`
`/opt/platform/apps/mongodb/dbroot`
`Checking that /dev/sdc1 is mounted`
`/backups`
`Application services:firewall processes stopped.`
`Reconfiguring applications...`
`Application insights-voss-sync processes started.`	

5. Single Node Upgrade

5.1. Upgrade a Single Node Cluster Environment with the ISO and Template

Important:

- Before upgrading to release 24.1:

  Install `EKB-21455-21.4.0_patch.script` first. Refer to `MOP-EKB-21455-21.4.0_patch.pdf`.

  - **Server Name**: https://voss.portalshape.com
  - **Path**: **Downloads > VOSS Automate > 24.1 > Upgrade > ISO**
  - **MOP**: MOP-EKB-21455-21.4.0_patch.pdf
  - **Patch File**: EKB-21455-21.4.0_patch.script

- Before upgrading to release 24.1, ensure that an additional 70 GB disk is available for the Insights database.

  See the Adding Hard Disk Space topic in the Platform Guide and VOSS Automate Hardware Specifications in the Architecture and Hardware Specification Guide.

  This disk is needed to assign to the `insights-voss-sync:database` mount point. See: *Mount the Insights disk (outside, after Maintenance Window)*.

- Before upgrading to release 24.1, ensure that sufficient time is allocated to the maintenance window. This may vary in accordance with your topology, number of devices and subscribers.

  The information below serves as a guideline VOSS support can be contacted if further guidance is required:

  - Cluster upgrade: 4h
  - Template install: 2.5h
  - For a 500K Data User system (13Mil RESOURCE documents), the expected `upgrade_db` step is about 12h.
  - For a 160K Data User system (2.5Mil RESOURCE documents), the expected `upgrade_db` step is about 2.5h.

  You can follow the progress on the Admin Portal transaction list.

- Tasks that are marked **Prior to Maintenance Window** can be completed a few days prior to the scheduled maintenance window so that VOSS support can be contacted if needed and in order to allow for reduce down time.

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

5.1.1. Download Files and Check (Prior to Maintenance Window)

Description and Steps	Notes and Status
VOSS files: **https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade** Download `.iso` and `.template` files, where XXX matches the release. Transfer the file to the `media/` folder. Two options: Either using SFTP: • **sftp platform@<unified_node_hostname>** • **cd media** • **put <upgrade_iso_file>** • **put <upgrade_template_file>** Or using SCP: • **scp <upgrade_iso_file> platform@<unified_node_ip_address>:~/media** • **scp <upgrade_template_file> platform@<unified_node_ip_address>:~/media** Verify that the `.iso` image and `.template` file copied: • **ls -l media/** Verify that the original `.sha256` checksums on the Download site match. • **system checksum media/<upgrade_iso_file>** `Checksum: <SHA256>` • **system checksum media/<upgrade_template_file>** `Checksum: <SHA256>`	

5.1.2. Security and Health Steps single node cluster (Prior to Maintenance Window)

Description and Steps	Notes and Status

The following step is needed if own private certificate and generated SAN certificates are required and the `web cert gen_csr` command was run. For details, refer to the Web Certificate Setup Options topic in the Platform Guide.
The steps below are needed to check if a CSR private key exists but no associated signed certificate is available.
Request VOSS support to run on the CLI as `root` user, the following command:
`for LST in /opt/platform/apps/nginx/config/csr/*;`
`do openssl x509 -in $LST -text -noout >/dev/null`
`2>&1 && SIGNED="$LST"; done`
 	
`echo $SIGNED`
If the `echo $SIGNED` command output is blank, back up the `csr/` directory with for example the following command:
`mv /opt/platform/apps/nginx/config/csr/ /opt/platform/apps/nginx/config/csrbackup`	

Description and Steps	Notes and Status
Validate the system health. Verify there are no pending Security Updates: **security check**	

Validate the system health. Carry out the following:
• **system mount** - mount upgrade ISO.
• **app install check_cluster** - install the new version of the **cluster check** command. For details, refer to the "Cluster Check" topic in the Platform Guide.
• **cluster check** - inspect the output of this command for warnings and errors. You can also use **cluster check verbose** to see more details, for example, `avx` enabled. While warnings will not prevent an upgrade, it is advisable that these be resolved prior to upgrading where possible. Some warnings may be resolved by upgrading. For troubleshooting and resolutions, also refer to the *Health Checks for Cluster Installations Guide* and *Platform Guide*.
If there is any sign of the paths below are over 80% full, a clean-up is needed, for example to avoid risk of full logs occurring during upgrade. Clean-up steps are indicated next to the paths:
`/ (call support if over 80%)`
`/var/log (run: log purge)`
`/opt/platform (remove any unnecessary files from /media directory)`
`/tmp (reboot)`
Verify there are no pending Security Updates.
--- 	
Note: If you run **cluster status** after installing the new version of **cluster check**, any error message regarding a failed command can be ignored. This error message will not show after upgrade.
--- 	
• **Adaptation check** - if the *GS SME Adaptation* is installed, check for duplicate instances of of `GS_SMETemplateData_DAT` and deleted any duplicates before upgrading to 24.1.	

5.1.3. Version Check (Prior to Maintenance Window)

Description and Steps	Notes and Status
Customized ``data/Settings`` If `data/Settings` 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 single node cluster (Maintenance Window)*. **Version** Record the current version information. This is required for upgrade troubleshooting. • Log in on the Admin Portal and record the information contained in the **About > Extended Version**	

5.1.4. Pre-Upgrade Steps single node cluster (Maintenance Window)

Description and Steps	Notes and Status

Choose an option:
• **If you're upgrading from: [21.4-PB4, 21.4-PB5]**
Place the system in maintenance mode to suspend any scheduled transactions. Scheduled transactions that are in progress will be allowed to complete, or otherwise, cancel data sync transactions that are in progress on the GUI. Refer to the Core Feature Guide. For details, refer to the System Maintenance Mode topic in the Platform Guide.
Run:
`cluster maintenance-mode start`
You can verify the maintenance mode status with:
`cluster maintenance-mode status`
• **If you're upgrading from: [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]**
Turn off any scheduled imports to prevent syncs triggering part way through the upgrade.
--- 	
Note: Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu available on the available on the `MVS-DataSync-Dashboard`.
--- 	
Two options are available:
Individually for each job:
1. Log in on the Admin Portal 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.
Mass modify:
1. On the Admin Portal, export scheduled syncs into a bulk load sheet.
2. Modify the schedule settings to de-activate scheduled syncs.
3. Import the sheet.
Schedules enabled on the CLI:
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>**.
Create a restore point and then restart server.
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. If you cannot restore the application from a restore point, your only recourse is to reinstall the application. When the backup is complete and you do not need the restore point for restore activities, you can remove it.
After the restore point has been created, restart.
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*.	

Description and Steps	Notes and Status
Before upgrading, check all services: Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on a fresh node. • **app status** Verify the node is not in the 'recovering' state (`stateStr` is not `RECOVERING`) • **database config**	

5.1.5. Upgrade single node cluster (Maintenance Window)

Note:

- By default, the cluster upgrade is carried out in parallel on all nodes and without any backup in order to provide a fast upgrade.
- For systems *upgrading to 24.1 from 21.4.0 - 21.4-PB5*:
  - The VOSS platform maintenance mode will be started automatically when the **cluster upgrade** command is run. This prevents any new occurrences of scheduled transactions, including the 24.1 database syncs associated with **insights sync**. For details on **insights sync**, see the *Insights Analytics* topic in the Platform Guide.
  - The **cluster maintenance-mode stop** command must however be run manually after the maintenance window of the upgrade: *End of the Maintenance Window and Restoring Schedules*.

For details on the VOSS platform maintenance mode, see the *Maintenance Mode* topic in the Platform Guide.

Description and Steps	Notes and Status

It is recommended that the upgrade steps are run in a terminal opened with the **screen** command.
On the primary unified node:
• **screen**
• **cluster upgrade media/<upgrade_iso_file>**
All unused docker images except `selfservice` and `voss_ubuntu` images will be removed from the system at this stage.
Note: If the system reboots, do not carry out the next manual reboot step.
To remove a mount directory `media/<iso_file basename>` on nodes that may have remained after for example an upgrade, run:
cluster run all app cleanup
Manual reboot *only if needed*:
• **system reboot**
If node messages: `<node name> failed with timeout` are displayed, these can be ignored.
Since all services will be stopped, this takes some time.
Close **screen**: `Ctrl-a \`
Log in on the primary database node and run **cluster run database app status**. If the report shows `insights-voss-sync:realtime stopped` on some database nodes, request assistance with root access on the system CLI from VOSS support in order to carry out the following on the primary database node:
1. Run the command:
`/opt/platform/mags/insights-voss-sync-mag-script install database`
This should return: `Configured Postgres secrets`.
2. Verify that the database nodes now all have the correct mongo info:
`cluster run database diag config app insights-voss-sync /mongo`
All nodes should have the password/port/user shown as below:
`mongo:`
`password: ********`
`port: 27020`
`user: insights-platform`
3. Restart the `insights-voss-sync:real-time` service on all database nodes:
`cluster run database app start insights-voss-sync:real-time`	

Note: In order to carry out fewer upgrade steps, the updates of instances of some models are skipped in the cases where:

- `data/CallManager` instance does not exist as instance in `data/NetworkDeviceList`
- `data/CallManager` instance exists, but `data/NetworkDeviceList` is empty
- Call Manager AXL Generic Driver and Call Manager Control Center Services match the `data/CallManager` IP

5.1.6. Post-Upgrade, Security and Health Steps single node cluster (Maintenance Window)

Description and Steps	Notes and Status
Verify the status: • **cluster check** • If any of the above commands show errors, check for further details to assist with troubleshooting: **cluster run all diag health** For a cloud deployment (MS Azure / AWS), also refer to the steps below.	
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.	

Complete all the security updates.
• **security update**
If upgrading a cloud deployment (MS Azure / AWS), run **cluster check**. If an error shows at each node:
`grub-pc: package in an undesired state`
then request assistance with root access on the system CLI from VOSS Support in order to run the command on each node:
`dpkg --configure -a`
A text user interface opens and you will be prompted:
– "GRUB install devices:"- Do *not* select any device. Press <Tab> to highlight <Ok> and press <Enter>.
– At "Continuing without installing GRUB?", press <Yes>
– Exit root user, run **cluster check** again and verify the error does not show.
The docker images `selfservice` and `voss_ubuntu` will be removed from the system at this stage.
Note: If the system reboots, do not carry out the next manual reboot step .
Manual reboot *only if needed*:
• **system reboot**	

5.1.7. Database Schema Upgrade single node cluster (Maintenance Window)

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. • **screen** • **voss upgrade_db**	

5.1.8. Template Upgrade single node cluster (Maintenance Window)

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. • **screen** • **app template media/<VOSS Automate.template>**	

The following message appears:

```
Running the DB-query to find the current environment's
existing solution deployment config...
```

- Python functions are deployed
- System artifacts are imported.

The template upgrade automatically detects the deployment mode, either “Enterprise” or “Provider”. A message displays according to the selected deployment type. Check for one of the messages below:

```
Importing EnterpriseOverlay.json

Importing ProviderOverlay.json ...
```

The template install automatically restarts necessary applications.

Description and Steps	Notes and Status

Review the output from the **app template** command and confirm that the upgrade message appears:
`Deployment summary of PREVIOUS template solution`
`(i.e. BEFORE upgrade):`
`------------------------------------------------`
`Product: [PRODUCT]`
`Version: [PREVIOUS PRODUCT RELEASE]`
`Iteration-version: [PREVIOUS ITERATION]`
`Platform-version: [PREVIOUS PLATFORM VERSION]`
This is followed by updated product and version details:
`Deployment summary of UPDATED template solution`
`(i.e. current values after installation):`
`------------------------------------------------`
`Product: [PRODUCT]`
`Version: [UPDATED PRODUCT RELEASE]`
`Iteration-version: [UPDATED ITERATION]`
`Platform-version: [UPDATED PLATFORM VERSION]`	

Description and Steps	Notes and Status
• If no errors are indicated, make a backup or restore point as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed. This restore point can be used if post-upgrade patches that may be required, fail.	

For an unsupported upgrade path, the install script stops with the message:
`Upgrade failed due to unsupported upgrade path.`
`Please log in as sysadmin`
`and see Transaction logs for more detail.`
You can restore to the backup or rollback/revert to the restore point made before the upgrade.	

If there are errors for another reason, the install script stops with a failure message listing the problem. Contact VOSS support.	
Post upgrade migrations: • **voss post-upgrade-migrations** Data migrations that are not critical to system operation can have significant execution time at scale. These need to be performed after the primary upgrade, allowing the migration to proceed whilst the system is in use - thereby limiting upgrade windows. A transaction is queued on VOSS Automate and its progress is displayed as it executes.	

Description and Steps	Notes and Status
Check status and health • **diag health** • **app status**	

5.1.9. Post Template Upgrade Tasks single node cluster (Maintenance Window)

Description and Steps	Notes and Status
Verify the upgrade: Log in on the Admin Portal and check the information contained in the **About > Version** menu. Confirm that versions have upgraded. • **Release** should show `XXX` • **Platform Version** should show `XXX` where `XXX` corresponds with the release number of the upgrade. If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again.	
• Check themes on all roles are set correctly	

5.1.10. Log Files and Error Checks single node cluster (Maintenance Window)

Description and Steps	Notes and Status
Inspect the output of the command line interface for upgrade errors, for example `File import failed!` or `Failed to execute command`. 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: `For more information refer to the execution log file with 'log view platform/execute.log'` For example, if it is required send all the install log files in the `install` directory to an SFTP server: • **log send sftp://x.x.x.x install**	
Log in on the Admin Portal as system level administrator, go to **Administration Tools > Transaction** and inspect the transactions list for errors.	

5.1.11. End of the Maintenance Window and Restoring Schedules

Description and Steps	Notes and Status
On the CLI: Run the **cluster maintenance-mode stop** command to end the VOSS maintenance mode when upgrading to 24.1 from 21.4 or 21.4.-PBx. This will allow scheduled data sync transactions to resume, including **insights sync** operations added in 24.1. For details on the VOSS platform maintenance mode, see the *Maintenance Mode* topic in the Platform Guide. • **If you're upgrading from: [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]** Restore Schedules --- **Note:** Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu available on the available on the `MVS-DataSync-Dashboard`. --- Re-enable scheduled imports if any were disabled prior to the upgrade. Individually for each job: 1. Log in on the Admin Portal 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. Mass modify: 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the sheet. --- **Note:** Select the **Skip next execution** option if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter. --- Schedules enabled on the CLI: For disabled schedules that were overlapping the maintenance window, enable. Run **schedule enable <job-name>**.	

5.1.12. Licensing (outside, after Maintenance Window)

Description and Steps	Notes and Status
From release 21.4 onwards, the deployment needs to be licensed. After installation, a 7-day grace period is available to license the product. Since license processing is only scheduled every hour, if you wish to license immediately, first run **voss check-license** on the CLI. 1. Obtain the required license token from VOSS. 2. a. To license through the GUI, follow steps indicated in Product License Management in the Core Feature Guide. b. To license through the CLI, follow steps indicated in Product Licensing in the Platform Guide.	

5.1.13. Mount the Insights disk (outside, after Maintenance Window)

Description and Steps	Notes and Status

On the primary unified node, assign the `insights-voss-sync:database` mount point to the drive added for the Insights database prior to upgrade.
For example, if `drives list` shows the added disk as:
`Unused disks:`
`sde`
then run the command
`drives add sde insights-voss-sync:database`
on each unified node where the drive has been added.
Sample output (the message below can be ignored on release 24.1:
`WARNING: Failed to connect to lvmetad. Falling back to device scanning.`)
`$ drives add sde insights-voss-sync:database`
`Configuration setting "devices/scan_lvs" unknown.`
`Configuration setting "devices/allow_mixed_block_sizes" unknown.`
`WARNING: Failed to connect to lvmetad. Falling back to device scanning.`
`71ad98e0-7622-49ad-9fg9-db04055e82bc`
`Application insights-voss-sync processes stopped.`
`Migrating data to new drive - this can take several minutes`
`Data migration complete - reassigning drive`
`Checking that /dev/sde1 is mounted`
`Checking that /dev/dm-0 is mounted`
`/opt/platform/apps/mongodb/dbroot`
`Checking that /dev/sdc1 is mounted`
`/backups`
`Application services:firewall processes stopped.`
`Reconfiguring applications...`
`Application insights-voss-sync processes started.`	

6. Upgrade Sheets

6.1. Multinode Upgrade Sheet

To download this sheet, refer to the HTML documentation.

Table 1: Multinode Upgrade Sheet

Description	Steps
Download Files and Check Steps	**Download Files and Check Steps**
**********	**********
Download VOSS files - XXX is the release number	https://voss.portalshape.com > **Downloads > VOSS Automate > XXX > Upgrade**
Download .iso and .template files	Transfer the .iso file to the media/ folder of all nodes
Download .iso and .template files	Transfer the .template file to the media/ folder of the primary node
Two transfer options:	
Either using SFTP:	
	sftp platform@<unified_node_hostname>
	cd media
	put <upgrade_iso_file>
	put <upgrade_template_file>
Or using SCP:	
	scp <upgrade_iso_file> platform@<unified_node_ip_address>:~/media
	scp <upgrade_template_file> platform@<unified_node_ip_address>:~/media
Verify that the .iso image and .template file copied:	**ls -l media/**
Verify that the original .sha256 checksums on the SFTP server match.	**system checksum media/<upgrade_iso_file>**
	`Checksum: <SHA256>`
	system checksum media/<upgrade_template_file>

continues on next page

Table 1 – continued from previous page

Description	Steps
	`Checksum: <SHA256>`
Security and Health Check Steps	**Security and Health Check Steps**
==================================	==================================
Verify that the primary node is the active primary node at the time of upgrade	**database config**
Ensure that the node on which the installation will be initiated has the stateStr parameter set to **PRIMARY** and has the **highest** priority **number** (highest priority number could vary depending on cluster layout)	Example output
	`<ip address>:27020: priority: <number> stateStr: PRIMARY storageEngine: WiredTiger`
Validate the system health.	**system mount** - mount the upgrade ISO.
	app install check_cluster - install the new version of the **cluster check** command.
For details: refer to the 'Cluster Check' topic in the Platform Guide.	
cluster check - inspect the output of this command for warnings and errors. You can also use **cluster check verbose** to see more details for example `avx` enabled. While warnings will not prevent an upgrade. It is advisable that these be resolved prior to upgrading where possible. Some warnings may be resolved by upgrading.	**cluster check**
For troubleshooting and resolutions: also refer to the *Health Checks for Cluster Installations Guide* and *Platform Guide*.	
If there is any sign of the paths below are over 80% full: a clean-up is needed. For example to avoid risk of full logs occurring during upgrade. Clean-up steps are indicated next to the paths:	
/	call support if over 80%
/var/log	run: **log purge**
/opt/platform	remove any unnecessary files from /media directory
/tmp	reboot
On the Primary Unified Node: verify there are no pending Security Updates on any of the nodes.	
Note: If you run **cluster status** after installing the new version of **cluster check**: any error message regarding a failed command can be ignored. This error message will not show after upgrade.	
Version Check steps	**Version Check steps**

continues on next page

Table 1 – continued from previous page

Description	Steps
==========	==========
Customized data/Settings	If data/Settings 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: Window Post Template Upgrade Tasks.	
Version	
Record the current version information. This is required for upgrade troubleshooting.	Log in on the Admin Portal and record the information contained in the **About > Extended Version**
Pre-Upgrade Steps	**Pre-Upgrade Steps**
==========	==========
VOSS cannot guarantee that a restore point can be used to successfully restore VOSS-4-UC. If you cannot restore the application from a restore point, your only recourse is to reinstall the application.	
Create a restore point as per the guidelines for the infrastructure on which the VOSS-4-UC platform is deployed.	
Optional: If a backup is also required	**backup add <location-name>**
	backup create <location-name>
For details, refer to the *Platform Guide*.	
After restore point creation and before upgrading: validate system health and check all services nodes and weights for the cluster:	**cluster run application cluster list**
Make sure all application nodes show 4 or 6 nodes.	**cluster check**
	inspect the output of this command, for warnings and errors. You can also use **cluster check verbose** to see more details.
	Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh unified nodes.
	Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster.
	Example output:
	172.29.21.240: weight: 80
	172.29.21.241: weight: 70
	172.29.21.243: weight: 60
	172.29.21.244: weight: 50

continues on next page

Table 1 – continued from previous page

Description	Steps
	Verify the primary node in the primary site and ensure no nodes are in the 'recovering' state (stateStr is not RECOVERING).
Upgrade steps	**Upgrade steps**
**********	**********
By default, the cluster upgrade is carried out in parallel on all nodes and without any backup in order to provide a fast upgrade.	
For systems upgrading to 24.1 from 21.4.0 – 21.4-PB5:	
The VOSS platform maintenance mode will be started automatically when the cluster upgrade command is run. This prevents any new occurrences of scheduled transactions, including the 24.1 database syncs associated with insights sync. For details on insights sync, see the Insights Analytics topic in the Platform Guide.	
The cluster maintenance-mode stop command must however be run manually after the maintenance window of the upgrade – see Manually Stop the Maintenance Window.	
For details on the VOSS platform maintenance mode, see the Maintenance Mode topic in the Platform Guide.	
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command.	
Verify that the ISO has been uploaded to the 'media/' directory on each node. This will speed up the upgrade time.	
On the primary unified node:	**screen**
	cluster upgrade media/<upgrade_iso_file>
Note: The **cluster upgrade** command will also silently first run **cluster check** and the upgrade will fail if any error conditions exist.	
Note: A check for security updates will also be made, with message 'Checking for security updates . . . '. If updates are found, a message will show the number and carry out the update. If no updates are found, a message 'No security updates found' shows.	
Note: If the system reboots, do not carry out the next manual reboot step.	

continues on next page

Table 1 – continued from previous page

Description	Steps
Manual reboot *only if needed*:	**cluster run notme system reboot**
If node messages: '<node name> failed with timeout' are displayed,these can be ignored.	**system reboot**
Since all services will be stopped, this takes some time.	
Post-Upgrade, Security and Health Steps	**Post-Upgrade, Security and Health Steps**
**********	**********
On the primary unified node, verify the 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**
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.	
Check for needed security updates. On the primary node, run:	**cluster run all security check**
Note: if the system reboots, do not carry out the next manual reboot step.	
Manual reboot only if needed:	**cluster run notme system reboot**
If node messages: <node name> failed with timeout are displayed, these can be ignored.	**system reboot**
Since all services will be stopped, this takes some time.	
Database Schema Upgrade steps	**Database Schema Upgrade steps**
**********	**********
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command.	On the primary unified node: **screen**
	voss upgrade_db
Check cluster status	**cluster check**
Template Upgrade steps	**Template Upgrade steps**
**********	**********
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command.	On the primary unified node: **screen**
	app template media/<VOSS-4-UC.template>
	Review the output from the **app template** command and confirm that the upgrade message appears.

continues on next page

Table 1 – continued from previous page

Description	Steps
	If no errors are indicated: make a backup or create a restore point as per the guidelines for the infrastructure on which the VOSS-4-UC platform is deployed. This restore point can be used if post-upgrade patches that may be required, fail.
For an unsupported upgrade path: the install script stops with the message:	
Upgrade failed due to unsupported upgrade path. Please log in as sysadmin and see Transaction logs for more detail.	You can restore to the backup or rollback, i.e. revert to the restore point made before the upgrade.
If there are errors for another reason: the install script stops with a failure message listing the problem.	Contact VOSS support.
Verify the 'extra_functions' have the *same checksum* across the cluster.	**cluster run application voss get_extra_functions_version -c**
Post upgrade migrations:	On a single node of a cluster: run: **voss post-upgrade-migrations**
Check cluster status and health	**cluster status**
Post Template Upgrade steps	**Post Template Upgrade steps**
**********	**********
Import device/cucm/PhoneType	
In order for a security profile to be available for a Call Manager Analog Phone, the 'device/cucm/PhoneType' model needs to be imported for each Unified CM.	1. Create a Model Type List which includes the 'device/cucm/PhoneType' 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.
Customized data/Settings	
	Merge the previously backed up customized 'data/Settings' 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.
Support for VG400 and VG450 Analogue Gateways	

continues on next page

Table 1 – continued from previous page

Description	Steps
Before adding the VG400 or VG450 Gateway, the 'device/cucm/GatewayType' model needs to be imported for each Unified CM.	1. Create a Model Type List which includes the 'device/cucm/GatewayType' 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.
Verify the upgrade	
	Log in on the Admin Portal and check the information contained in the **About > Version** menu. Confirm that versions have upgraded.
	Release should show 'XXX', where this matches the upgrade release.
	Check themes on all roles are set correctly
	For configurations that make use of the Northbound Billing Integration (NBI): please check the service status of NBI and restart if necessary.
Log Files and Error Checks	**Log Files and Error Checks**
**********	**********
Inspect the output of the command line interface for upgrade errors - for example: File import failed! or Failed to execute command.	
To view any log files indicated in the error messages - for example run the command if the following message appears:	**log view**
For more information refer to the execution log file with log view platform/execute.log	
If it is for example required send all the install log files in the install directory to an SFTP server:	**log send sftp://x.x.x.x install**
Log in on the Admin Portal as system level administrator	Go to **Administration Tools > Transaction** and inspect the transactions list for errors
Manually Stop the Maintenance Window	**Manually Stop the Maintenance Window**
**********	**********
On the CLI:	**cluster maintenance-mode stop**

continues on next page

Table 1 – continued from previous page

Description	Steps
Run the **cluster maintenance-mode stop** command to end the automatic start of the VOSS maintenance mode when the cluster upgrade command was run when upgrading to 24.1 from 21.4.0 - 21.4-PB5.	
This will allow synced transactions to resume, including insights sync operations added in 24.1.	
For details on the VOSS platform maintenance mode, see the Maintenance Mode topic in the Platform Guide.	
Licensing (outside, after Maintenance Window)	**Licensing (outside, after Maintenance Window)**
==========	**==========**
From release 21.4 onwards, the deployment needs to be licensed. After installation, a 7-day grace period is available to license the product. Since license processing is only scheduled every hour, if you wish to license immediately, first run **voss check-license** from the primary unified node CLI.	**voss check-license**
Obtain the required license token from VOSS.	
Steps for GUI and CLI:	
To license through the GUI, follow steps indicated in Product License Management in the Core Feature Guide.	
To license through the CLI, follow steps indicated in Product Licensing in the Platform Guide.	
Mount the Insights disk (outside, after Maintenance Window)	**Mount the Insights disk (outside, after Maintenance Window)**
==========	**==========**
On each unified node, assign the insights-voss-sync:database mount point to the drive added for the Insights database prior to upgrade.	
For example, if drives list shows the added disk as: Unused disks: sde	For example, if drives list shows the added disk as: Unused disks: sde
drives add sde insights-voss-sync:database	**drives add sde insights-voss-sync:database**
the message below can be ignored on release 24.1:	

continues on next page

Table 1 – continued from previous page

Description	Steps
WARNING: Failed to connect to lvmetad. Falling back to device scanning.	

Index